



# Alcatel-Lucent 5450

IP Session Control | Release 22.1

**Provisioning Guide**

9YZ-04666-AAAI-TCZZA

Issue 0.02 | June 2012

**Alcatel-Lucent - Proprietary**  
Use pursuant to applicable agreements

**Legal notice**

Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Copyright © 2012 Alcatel-Lucent. All rights reserved.

Contains proprietary/trade secret information which is the property of Alcatel-Lucent and must not be made available to, or copied or used by anyone outside Alcatel-Lucent without its written authorization.

Not to be used or disclosed except in accordance with applicable agreements.

**Notice**

Every effort has been made to ensure that the information contained in this information product was accurate at the time of printing. However, information is subject to change.

**Conformance statements**

See [Chapter 11, “Conformance statements”](#).

**Security statement**

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of remote access features. In such an event, applicable tariffs require that the customer pay all network charges for traffic. Alcatel-Lucent cannot be responsible for such charges and will not make any allowance or give any credit for charges that result from unauthorized access.

**Limited Warranty**

For terms and conditions of sale, contact your Alcatel-Lucent Account Team.

**Licenses**

For information on the product license statements for open source software, refer the document, *Free and Open Source Software Copyright Notice and Licenses*, 270-702-028R5.1.

**Developed by Alcatel-Lucent.**

# Contents

## About this document

|   |       |
|---|-------|
| Purpose .....   | xxiii |
| Document changes from the previous software release ..... | xxiii |
| Safety information .....                                  | xxiii |
| Intended audience .....                                   | xxiii |
| How to use this information product .....                 | xxiv  |
| Conventions used .....                                    | xxiv  |
| Systems supported .....                                   | xxiv  |
| Related documentation .....                               | xxiv  |
| Alcatel-Lucent 5450 ISC training .....                    | xxv   |
| Tasks .....   | xxv   |
| Document support .....                                    | xxvi  |
| Technical support .....                                   | xxvi  |
| How to order .....  | xxvi  |
| How to comment .....                                      | xxvi  |

## Part I: Provisioning task flows

### 1 ISC

|                |     |
|----------------|-----|
| Overview ..... | 1-1 |
|----------------|-----|

#### IMS components

|   |      |
|---|------|
| Overview .....                              | 1-4  |
| IP Session Control configuration flow ..... | 1-5  |
| S-CSCF provisioning task flow .....         | 1-7  |
| I-CSCF provisioning taskflow .....          | 1-12 |

---

|   |      |
|---|------|
| P-CSCF provisioning task flow .....   | 1-15 |
| BGCF provisioning task flow .....   | 1-19 |
| IBCF provisioning task flow .....   | 1-23 |
| E-CSCF provisioning taskflow .....  | 1-25 |
| NTM provisioning task flow .....  | 1-27 |
| EEAS provisioning task flow .....   | 1-28 |
| IMS-GWF provisioning task flow .....  | 1-30 |
| iAGCF provisioning taskflow .....   | 1-33 |
| SIP Permanent Linksets provisioning taskflow .....                                  | 1-35 |
| Provision Diameter connection interface to support Multiple Destination FQDNs ..... | 1-36 |
| <b>Services</b>   |      |
| Overview .....  | 1-38 |
| To provision SIP forking .....  | 1-40 |
| Provisioning Task flow - To provision Early IMS Security provisioning .....         | 1-41 |
| Provisioning Task flow - To provision NASS-bundled authentication .....             | 1-43 |
| Symmetric TCP connections provisioning taskflow .....                               | 1-45 |
| To provision inter-working of media between IPv4 and IPv6 networks .....            | 1-46 |
| Provisioning Task flow - To provision SIP Message Screening .....                   | 1-47 |
| Provisioning Task flow - To provision Priority Mode .....                           | 1-49 |
| Provision Integrated Security Gateway (iSGW) .....                                  | 1-51 |
| Provision P-CSCF support of generating ACRs for emergency calls .....               | 1-53 |
| Digit Analysis and Normalization Function - Provisioning Task flow .....            | 1-55 |
| ICSI provisioning task flow .....   | 1-57 |
| Provision Bearer Statistics Collection on iAGCF .....                               | 1-59 |
| Provision the support of session and bandwidth limits per enterprise/PBX .....      | 1-60 |
| Provision the Signaling Firewall .....  | 1-62 |

|  |       |
|--|-------|
| Signaling Firewall Load Balancer or Distribution Function with Single IP Address Exposed for the Gm Interface to End Users - Provisioning Taskflow ..... | 1-64  |
| Cx Enhancement to support SIP Digest per 3GPP R8 - Provisioning task flow .....  | 1-66  |
| Provisioning Cx Enhancement per 3GPP R7 and R8 .....   | 1-68  |
| Provision Common Announcement Module (CANM) task flow .....  | 1-69  |
| BGCF support for Digit Manipulation provisioning task flow .....   | 1-73  |
| Provision iAGCF support of Network Traffic Management (NTM) .....  | 1-75  |
| CMCC Emergency Service and P-CSCF SIP Header Manipulation provisioning task flow .....   | 1-78  |
| Support.sending.offline.charging.data.to.the.CCF.provisioned.to.the.CTS.-.Provisioning.task.flow.....  | 1-80  |
| Limit for TCP Connections - Provisioning .....   | 1-82  |
| Enhancement of Rx and Gq' interfaces - Provisioning .....  | 1-83  |
| Allow SIPS-URI on Gm and Mw Interface - Provisioning .....   | 1-84  |
| IMUX provisioning task flow .....  | 1-88  |
| Provisioning Support of the NENA V5 SIP Interface to LRF and EATF for SRVCC .....  | 1-92  |
| Provisioning - Support MSRP Peak Data Rate to Enhance User Experience .....  | 1-94  |
| Provisioning - iAGCF Support of a Large Number of Residential Gateways .....   | 1-96  |
| Provisioning the border access capability for H.248 interface .....  | 1-100 |
| Access border for IMS or Pre-IMS core provisioning task flow .....   | 1-104 |
| Provisioning Task flow - To provision S-CSCF Assisted Relocation Procedure for Geo-Redundancy Enhancement .....  | 1-118 |
| Provisioning Task flow - To provision iAGCF Line OOS and CPC Display functionalities .....   | 1-119 |
| To provision ATCF support .....  | 1-121 |
| Provisioning Task flow - To provision SIP heartbeat after failure to reach a network element .....   | 1-123 |
| Provisioning task flow - To provision primary and alternate SLF destination for geo-redundancy support .....   | 1-125 |
| Provisioning Task flow - To support new versions of IMS charging SPEC 3GPP 32.260 .....  | 1-127 |

|                |     |
|----------------|-----|
| Overview ..... | 2-1 |
|----------------|-----|

**3GPP2 SBBC**

|   |     |
|---|-----|
| Overview .....                                  | 2-2 |
| 3GPP2 SBBC provisioning task flow .....         | 2-3 |
| PD-FE 3GPP2 policy provisioning task flow ..... | 2-6 |

**TISPAN RACS**

|  |      |
|--|------|
| Overview .....                                   | 2-8  |
| TISPAN RACS provisioning task flow .....         | 2-9  |
| PD-FE TISPAN policy provisioning task flow ..... | 2-15 |
| Media Inactivity provisioning task flow .....    | 2-16 |

**3 Offline charging**

|   |     |
|---|-----|
| Overview .....  | 3-1 |
| <b>ACR and ABF provisioning task flows</b>                |     |
| Overview .....  | 3-2 |
| Provision ACR task flow .....                             | 3-3 |
| ACR Buffering Function (ABF) provisioning task flow ..... | 3-5 |

**Part II: IP session control (ISC) configuration****4 Manage system configuration**

|   |      |
|---|------|
| Overview .....  | 4-1  |
| <b>S-CSCF provisioning</b>  |      |
| Overview .....  | 4-5  |
| To provision SDP media .....                                      | 4-6  |
| To provision an S-CSCF profile .....                              | 4-15 |
| To provision Emergency Session Routing Method .....               | 4-26 |
| To provision support for wildcard PUID .....                      | 4-27 |
| To activate PacketCable authentication in an S-CSCF profile ..... | 4-29 |
| To provision a S-CSCF PSI URI table .....                         | 4-31 |

**Contents**

|  |       |
|--|-------|
| To provision a Home Network Identifier profile table .....         | 4-33  |
| To activate enhanced third party registration .....                | 4-35  |
| To provision the S-CSCF profile to support IP-PBX calls .....      | 4-36  |
| Provisioning Task flow - To provision S-CSCF pool .....            | 4-40  |
| <b>I-CSCF provisioning</b>   |       |
| Overview .....   | 4-44  |
| To provision ICSCF Profile .....                                   | 4-45  |
| To provision the S-Cscf Capability List .....                      | 4-53  |
| To create a PSI sub-domain list .....                              | 4-57  |
| <b>P-CSCF provisioning</b>   |       |
| Overview .....   | 4-61  |
| To provision a Session Description Protocol Profile .....          | 4-62  |
| To provision Service-Based PCSCF Profile .....                     | 4-69  |
| To provision SIP Stack Timer Profile .....                         | 4-74  |
| To provision PCSCF profile .....                                   | 4-77  |
| To provision PBX Table Entry .....                                 | 4-96  |
| To activate the SIP header reduction .....                         | 4-101 |
| To activate Service Route header .....                             | 4-102 |
| To activate PacketCable authentication in the P-CSCF profile ..... | 4-104 |
| To provision SIP compression .....                                 | 4-106 |
| To provision IMS Signaling security .....                          | 4-108 |
| To provision the Service Based Local Policy Profile .....          | 4-111 |
| To provision e2 interface support .....                            | 4-116 |
| Support to provide P-CSCF IP address to UE .....                   | 4-120 |
| To provision the TLS Profile table .....                           | 4-121 |
| To provision the SIP Error Treatment Table attributes .....        | 4-123 |
| Provisioning Task flow - To provision P-CSCF pool .....            | 4-126 |

**BGCF provisioning**

|  |       |
|--|-------|
| Overview .....   | 4-132 |
| To provision BGCF URI Id .....                                     | 4-133 |
| To provision BGCF Target List .....                                | 4-138 |
| To provision BGCF Profile .....                                    | 4-142 |
| To provision BGCF Time Of Day .....                                | 4-148 |
| To provision BGCF Network Gateway .....                            | 4-152 |
| To provision BGCF Default Network Gateway .....                    | 4-156 |
| To provision Originating Host Class Profile routing for BGCF ..... | 4-160 |
| To provision Subscriber Profile routing for BGCF .....             | 4-163 |
| To provision BGCF DA Route Table .....                             | 4-172 |
| To provision BGCF SIP content type .....                           | 4-177 |
| To provision BGCF local number routing .....                       | 4-181 |
| To provision BGCF location based routing .....                     | 4-189 |
| To provision BGCF Originating Host ID .....                        | 4-193 |

**IBCF provisioning**

|                                 |       |
|---------------------------------|-------|
| Overview .....                  | 4-197 |
| To provision IBCF Profile ..... | 4-198 |

**E-CSCF provisioning**

|   |       |
|---|-------|
| Overview .....                                      | 4-204 |
| Emergency provisioning scenarios .....              | 4-205 |
| To provision IMS Emergency Service Identifier ..... | 4-208 |
| To provision an E-CSCF Profile table .....          | 4-212 |

**NTM provisioning**

|   |       |
|---|-------|
| Overview .....                          | 4-221 |
| To provision an NTM Control table ..... | 4-222 |

|  |       |
|--|-------|
| To provision an NTM Exemption table .....                                      | 4-226 |
| To provision an I-CSCF profile table .....                                     | 4-230 |
| <b>EEAS provisioning</b>   |       |
| Overview .....   | 4-237 |
| To provision an E.164 Expansion AS profile .....                               | 4-238 |
| <b>IMS gateway function provisioning</b>                                       |       |
| Overview .....   | 4-241 |
| To provision Online Charging Trigger Data table .....                          | 4-242 |
| To provision MRF Announcement Interface profile .....                          | 4-245 |
| To provision MRF Announcement Data table .....                                 | 4-247 |
| To provision IGWF profile .....  | 4-250 |
| <b>P-NAPTR provisioning</b>  |       |
| Overview .....   | 4-252 |
| To provision a P-NAPTR Region .....  | 4-253 |
| To provision a P-NAPTR Target URI .....  | 4-257 |
| <b>iAGCF provisioning</b>  |       |
| Overview .....   | 4-260 |
| Introduction to the base configuration .....                                   | 4-261 |
| <b>SIP permanent linksets provisioning</b>                                     |       |
| Overview .....   | 4-263 |
| To provision an SIP Linkset .....  | 4-264 |
| To provision an SIP Permanent Linkset Group .....                              | 4-269 |
| <b>Provisioning diameter multiple destination FQDNs</b>                        |       |
| Overview .....   | 4-272 |
| Conversion from Diameter Geo-redundancy to support Multiple destinations ..... | 4-273 |
| Conversion from Multiple destination to support Diameter Geo-redundancy .....  | 4-276 |

---

|  |       |
|--|-------|
| To provision a Diameter Multiple Destination Profile .....                 | 4-278 |
| <b>Border gateway provisioning</b>   |       |
| Overview .....   | 4-282 |
| To provision a Core Bearer Realm .....                                     | 4-283 |
| To provision a Published Realm .....                                       | 4-286 |
| To assign a Published Realm to a Border Gateway .....                      | 4-290 |
| <b>Central Routing Function provisioning</b>                               |       |
| Overview .....   | 4-293 |
| CRF provisioning task flow .....   | 4-294 |
| To provision a CRF Target table .....                                      | 4-297 |
| To provision a CRF Target List table .....                                 | 4-302 |
| To provision a CRF Treatment table .....                                   | 4-306 |
| To provision a CRF Digit Analysis Table .....                              | 4-310 |
| To provision a CRF Trunk Group table .....                                 | 4-313 |
| To provision a CRF Route Plan table .....                                  | 4-316 |
| To provision a CRF Task Plan table .....                                   | 4-320 |
| To provision a CRF Route Priority List table .....                         | 4-324 |
| To provision a CRF Route Profile table .....                               | 4-328 |
| <b>5 Manage services</b>   |       |
| Overview .....   | 5-1   |
| <b>To provision nomadic access</b>   |       |
| Overview .....   | 5-6   |
| To enable/disable nomadic user access .....                                | 5-7   |
| <b>To provision the geographic location service for VoWLAN subscribers</b> |       |
| Overview .....   | 5-8   |
| To provision a MACaddress to Location table .....                          | 5-9   |

**Contents**

|   |      |
|---|------|
| To provision a Map Special Code to Dialed Number .....                    | 5-11 |
| To provision Geographic Location Server .....                             | 5-13 |
| To provision client access to the Geographic Location Server .....        | 5-15 |
| <b>To provision multiple home domains</b>                                 |      |
| Overview .....  | 5-17 |
| To provision multiple home domains .....                                  | 5-18 |
| <b>To provision IMS roaming</b>   |      |
| Overview .....  | 5-20 |
| To provision IMS roaming .....  | 5-21 |
| <b>To provision SIP message screening</b>                                 |      |
| Overview .....  | 5-22 |
| To provision an SIP Filter .....  | 5-23 |
| To provision an SIP Filter Header Rule .....                              | 5-28 |
| To provision an SIP Filter Body Rule .....                                | 5-36 |
| To provision an SIP Filter Reference Rule .....                           | 5-44 |
| To provision an SIP Filter Parameter Rule .....                           | 5-50 |
| To provision an SIP Filter Set .....                                      | 5-57 |
| <b>To provision priority mode</b>   |      |
| Overview .....  | 5-60 |
| To provision an Emergency Identifiers List .....                          | 5-61 |
| To provision an NGN GETS Identifier List .....                            | 5-64 |
| <b>To provision security gateway</b>                                      |      |
| Overview .....  | 5-67 |
| To provision an SIP Flow Trusted/Untrusted Rate Limit Rule Set .....      | 5-68 |
| To provision an SIP Aggregate Trusted/Untrusted Rate Limit Rule Set ..... | 5-72 |
| To provision a Flow Source Address Policy .....                           | 5-76 |

---

|  |       |
|--|-------|
| To provision an Aggregate Source Address Policy .....                              | 5-80  |
| To provision a Registration Failure Policy .....                                   | 5-83  |
| To provision an Application Layer Policy .....                                     | 5-87  |
| To provision a Security Gateway Profile .....                                      | 5-90  |
| <b>To provision support of digit analysis and normalization function</b>           |       |
| Overview .....   | 5-94  |
| Introduction to Digit Analysis (DA) tables .....                                   | 5-95  |
| Digit Analysis (DA) Rules .....  | 5-98  |
| Digit Analysis (DA) Rules -BGCF .....  | 5-105 |
| To provision a SIP Error Code table .....  | 5-106 |
| To provision an IMS Digit Table .....  | 5-110 |
| <b>To provision ICSI</b>   |       |
| Overview .....   | 5-116 |
| To provision an ICSI profile .....   | 5-117 |
| <b>To provision bearer statistics collection on the iAGCF</b>                      |       |
| Overview .....   | 5-122 |
| Support collecting Bearer statistics at AGCF from Access GW .....                  | 5-123 |
| <b>To provision the support of session and bandwidth limits per enterprise/PBX</b> |       |
| Overview .....   | 5-124 |
| To provision a Virtual Group profile .....   | 5-125 |
| To provision a Service Level Policy .....  | 5-129 |
| To provision the IBC-A VG Policy .....   | 5-133 |
| To provision a VG and Service Mapping Profile .....                                | 5-137 |
| <b>To provision signaling firewall</b>   |       |
| Overview .....   | 5-141 |
| To provision FEPH Flow Policy .....  | 5-142 |

*Contents*

|   |       |
|---|-------|
| Provision an Aggregate Packet Policy .....                          | 5-147 |
| Provision an Aggregate Flow Policy .....                            | 5-150 |
| Provisioning task flow for hardware acceleration .....              | 5-151 |
| Provision an Aggregate Policy Assignment .....                      | 5-154 |
| To provision an IPsec Parameters table .....                        | 5-155 |
| <b>Signaling Firewall configuration</b>                             |       |
| Overview .....  | 5-159 |
| External subnets .....  | 5-160 |
| Published NI IP addresses for FEPH and IMS services .....           | 5-161 |
| Default gateway and/or static routes for IMS services .....         | 5-162 |
| <b>IMS Service Growth with an existing FEPH Service</b>             |       |
| Overview .....  | 5-163 |
| To grow an IMS service that is FEPH-enabled .....                   | 5-164 |
| To disable FEPH on an FEPH-enabled IMS service .....                | 5-166 |
| To add FEPH IPv4 or IPv6 capability for an IMS service .....        | 5-167 |
| To remove FEPH IPv4 or IPv6 capability for an IMS service .....     | 5-170 |
| <b>Signaling Firewall Service Growth with existing IMS Services</b> |       |
| Overview .....  | 5-172 |
| Signaling Firewall growth preparation and planning .....            | 5-173 |
| To grow Signaling Firewall and FEPH on an existing network .....    | 5-179 |
| To grow Signaling Firewall and FEPH on a new network .....          | 5-191 |
| FEPH growth cleanup .....   | 5-200 |
| Service growth of FEPH service on HSPP4 of Malban (Hub) card .....  | 5-201 |
| fephGrowth command .....  | 5-208 |
| FEPH growth error-handling .....                                    | 5-211 |
| FEPH growth worksheet .....   | 5-212 |

---

|  |       |
|--|-------|
| <b>Migration procedure for signaling firewall load balancer/distribution function</b>  |       |
| Overview .....   | 5-222 |
| Migration Procedure for Signaling Firewall Load Balancer/Distribution Function .....   | 5-223 |
| <b>To provision signaling firewall load balancer or distribution function with single IP address exposed for the Gm interface to end users</b> |       |
| Overview .....   | 5-229 |
| To provision a Published NI Group Assignment table .....   | 5-230 |
| <b>To provision common announcement module (CANM)</b>  |       |
| Overview .....   | 5-235 |
| To provision a Treatment Trigger Data Table .....  | 5-236 |
| To provision a CANM Profile Table .....  | 5-239 |
| <b>To provision iAGCF support of network traffic management (NTM)</b>  |       |
| Overview .....   | 5-245 |
| To provision an AGCF Cause Code To H248 Tone Table .....   | 5-246 |
| <b>To provision CMCC emergency service and P-CSCF SIP header manipulation</b>  |       |
| Overview .....   | 5-249 |
| To provision an Access Location to ESRN Mapping Table .....  | 5-250 |
| To provision an IP Address Mapping Table .....   | 5-255 |
| To provision a Default Access Location Table .....   | 5-259 |
| <b>To provision support for sending offline charging data to the CCF provisioned to the CTS</b>  |       |
| Overview .....   | 5-263 |
| Support sending offline charging data to the CCF provisioned to the CTS .....  | 5-264 |
| <b>To provision limit for TCP connections</b>  |       |
| Overview .....   | 5-265 |
| To provision a Remote IP Policy Table .....  | 5-266 |
| <b>To provision IMUX services</b>  |       |
| Overview .....   | 5-270 |

|  |       |
|--|-------|
| To provision IMUX to IMS Association Table .....                           | 5-271 |
| To provision IMUX port .....   | 5-274 |
| <b>To provision iHSS/iSLF support of per-enterprise domains</b>            |       |
| Overview .....   | 5-279 |
| iHSS/iSLF support of per-enterprise domains .....                          | 5-280 |
| Provisioning the Subscriber Home Domain Table .....                        | 5-281 |
| <b>To provision MSRP peak data rate support to enhance user experience</b> |       |
| Overview .....   | 5-285 |
| To provision an SDP Media MSRP Table .....                                 | 5-286 |
| <b>To provision access border for IMS or pre-IMS core</b>                  |       |
| Overview .....   | 5-289 |
| To provision IBC-A Profile .....   | 5-290 |
| To provision IBC Route Profile .....                                       | 5-297 |
| To provision Target Group Table .....                                      | 5-304 |
| To provision Target Group List .....                                       | 5-310 |
| To provision IBC Domain Table .....  | 5-314 |
| To provision Trunk Group .....   | 5-318 |
| To provision ACL List .....  | 5-322 |
| <b>To provision iAGCF line OOS and CPC display functionalities</b>         |       |
| Overview .....   | 5-327 |
| To provision an AGCF CPC String to CPC Digit Table .....                   | 5-328 |
| <b>To provision Access Transfer Control Function (ATCF) support</b>        |       |
| Overview .....   | 5-331 |
| To provision an STN-SR Table .....   | 5-332 |
| <b>To provision SIP heartbeat after failure to reach a network element</b> |       |
| Overview .....   | 5-336 |

---

|   |       |
|---|-------|
| To provision an SIP Heartbeat after failure Exemption Table ..... | 5-337 |
|---|-------|

## **Support Multiple Access Network Subnets on FEPH**

|  |       |
|--|-------|
| Overview .....   | 5-341 |
| Support multiple access network subnets on FEPH .....          | 5-342 |
| To grow a new external access subnet .....                     | 5-343 |
| To convert one ordinary subnet to external access subnet ..... | 5-360 |
| To degrow one external access subnet .....                     | 5-371 |

**6**

## **Translations**

|                |     |
|----------------|-----|
| Overview ..... | 6-1 |
|----------------|-----|

### **BGCF Translations**

|                                    |     |
|------------------------------------|-----|
| Overview .....                     | 6-2 |
| BGCF translations .....            | 6-3 |
| BGCF CIC dialing prefix .....      | 6-4 |
| BGCF per-carrier translation ..... | 6-5 |
| BGCF sample translations .....     | 6-6 |

## **Part III: Service policy decision function (SPDF) configuration**

**7**

### **Manage system configuration**

|                |     |
|----------------|-----|
| Overview ..... | 7-1 |
|----------------|-----|

#### **3GPP2 SBBC**

|  |      |
|--|------|
| Overview .....                             | 7-2  |
| To provision a Subscriber Tier table ..... | 7-3  |
| To provision an IP Filter table .....      | 7-6  |
| To provision a Rule Name table .....       | 7-11 |
| To provision a PCC Rule table .....        | 7-14 |
| To provision a Rule Name List table .....  | 7-20 |
| To provision a Policy Selector Table ..... | 7-24 |

**Contents**


---

|   |      |
|---|------|
| <b>TISPAN RACS</b>  |      |
| Overview .....  | 7-28 |
| To add an H.248 Device Server .....                                       | 7-29 |
| To provision an H.248-controlled BGW .....                                | 7-32 |
| To provision a DSCP Profile table .....                                   | 7-36 |
| <br><b>Part IV: Accounting management</b>                                 |      |
| <b>8     Offline charging</b>   |      |
| Overview .....  | 8-1  |
| <b>Provision ACR task flow</b>  |      |
| Overview .....  | 8-2  |
| To activate an ACR message generation on a SIPia port .....               | 8-3  |
| To provision an ACR Charging Profile .....                                | 8-5  |
| Assigning an ACR Charging profile to an IMS entity .....                  | 8-15 |
| ACR Consolidation Enhancement .....                                       | 8-18 |
| <b>Provision ACR buffering function</b>                                   |      |
| Overview .....  | 8-20 |
| ACR Buffering Function (ABF) .....  | 8-21 |
| To provision an ABF Diameter profile table .....                          | 8-24 |
| <b>Miscellaneous topics</b>   |      |
| Overview .....  | 8-29 |
| Activate inclusion of CDMA access network information .....               | 8-30 |
| Checking compatibility with 3GPP Release 7 Diameter messages on CCF ..... | 8-31 |
| <b>9     Online charging</b>  |      |
| Overview .....  | 9-1  |
| <b>Online charging procedures</b>   |      |
| Overview .....  | 9-2  |

---

|   |     |
|---|-----|
| To provision an Online Charging Profile table ..... | 9-3 |
| Provision S-CSCF profile for online charging .....  | 9-7 |

## **Part V: Common procedures for ISC and SPDF**

### **10 Common procedures**

|                |      |
|----------------|------|
| Overview ..... | 10-1 |
|----------------|------|

#### **IP session control and service policy decision function**

|  |       |
|--|-------|
| Overview .....   | 10-3  |
| To connect to the CNFG host using the Provisioning GUI ..... | 10-4  |
| To execute the base configuration .....                      | 10-6  |
| To start and verify the FSDB .....                           | 10-8  |
| To provision NGSS Server parameters .....                    | 10-9  |
| To provision an IMS Service association .....                | 10-20 |
| To provision a Diameter profile .....                        | 10-23 |
| To modify Diameter application IDs .....                     | 10-31 |
| To provision a Service to Diameter mapping .....             | 10-32 |

#### **IP session control**

|   |       |
|---|-------|
| Overview .....  | 10-36 |
| To provision an SCTP Profile .....                                      | 10-37 |
| To provision a SIPia port .....   | 10-40 |
| To provision ENUM server addresses .....                                | 10-49 |
| To provision an incoming digit table .....                              | 10-50 |
| To provision the ENUM profile .....                                     | 10-57 |
| To provision an Originating Hosts list .....                            | 10-64 |
| Wildcards in digit strings .....  | 10-68 |
| To change the operational state of a host providing IMS Service .....   | 10-72 |
| To change the operational or administrative state of a SIPia port ..... | 10-80 |

**Contents**

|   |        |
|---|--------|
| To view the operational state of a host providing IMS Service ..... | 10-82  |
| To view the administrative state of a SIPia port .....              | 10-83  |
| Verifying operational functionality using the ims_cli command ..... | 10-84  |
| To provision an External Domain Routing table .....                 | 10-99  |
| <b>Service policy decision function</b>                             |        |
| Overview .....  | 10-103 |
| To provision a PDF profile .....                                    | 10-104 |
| To provision a Diameter port .....                                  | 10-108 |
| To lock, or unlock a Diameter port .....                            | 10-111 |
| To provision a variant .....  | 10-114 |
| To provision a PPL component in a signaling variant .....           | 10-116 |
| <b>Part VI: Conformance and hazard statements</b>                   |        |
| <b>11 Conformance statements</b>                                    |        |
| Overview .....  | 11-1   |
| 5400 LCP compliance summary .....                                   | 11-2   |
| Eco-environmental statements .....                                  | 11-3   |
| <b>12 Hazard statements</b>   |        |
| Overview .....  | 12-1   |
| Structure of safety statements .....                                | 12-2   |
| Common cautions and warnings .....                                  | 12-4   |
| Basic safety aspects .....  | 12-6   |
| <b>A Sample output for fehgrowth -m</b>                             |        |
| Overview .....  | A-1    |
| <b>B References</b>   |        |
| Overview .....  | B-1    |

---

|                       |     |
|-----------------------|-----|
| Reissue history ..... | B-2 |
|-----------------------|-----|

**Glossary****Index**

# List of tables

B-1      Issue 0.02, June 2012 ..... B-2



# About this document

## Purpose

The purpose of this information product is to provide task flows and procedures to perform configuration management and accounting management tasks.

The 5450 IP Session Control (ISC) application can be deployed on different hardware platforms. Therefore, use this information product in conjunction with the appropriate platform documentation.

*Note :* This document does not cover the initial installation and provisioning of the equipment. Installation and provisioning is typically performed by Alcatel-Lucent personnel.

## Document changes from the previous software release

This is the final draft issue of the document for Release 22.1. See [Appendix B, “References”](#) for the Release 22.1 changes.

## Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

## Intended audience

The audience for this information product includes:

- Maintenance technician
- Maintenance specialist
- Operator
- Administrator

## How to use this information product

This Information Product is intended to be used as reference for the 5450 IP Session Control (ISC) application. To perform tasks may require the access to specific vendor documents, which are referred in the different procedures.

## Conventions used

The following summarizes presentation conventions.

| Convention                 | Information Type              |
|----------------------------|-------------------------------|
| output                     | A system output message       |
| <b>cd /bin</b>             | A command entered by the user |
| <b>Enter</b>               | Keyboard entries              |
| <b>&lt;IP Address&gt;</b>  | Variable parameters           |
| <i>filename</i>            | File name                     |
| <b>Tools-&gt;Discovery</b> | User interface string         |
| APx                        | Variable entities             |

## Systems supported

This version of the document applies to the IMS Release 11.1.

## Related documentation

The following manuals are available:

- *Alcatel-Lucent 5450 IP Session Control Application User Guide*, 275-900-361
- *Alcatel-Lucent 5450 IP Session Control Alarm Dictionary*, 270-702-032
- *Alcatel-Lucent 5450 IP Session Control CALEA/Lawful Intercept Technical Description and Provisioning*, 275-100-049
- *Alcatel-Lucent 5450 IP Session Control Software Licenses*, 270-702-029
- *Alcatel-Lucent 5450 IP Session Control Alarm, Performance Measurement, System Parameters, Ports, Protocols and MIB release differences*, 270-900-878
- *Alcatel-Lucent 5400 Linux Control Platform Charging Interface Specification*, 275-900-393
- *Alcatel-Lucent 5420 Converged Telephony Server (CTS) Application User Guide*, 275-900-366
- *Alcatel-Lucent 5400 Linux Control Platform System Guide*, 270-702-011
- *Alcatel-Lucent 5400 Linux Control Platform Hardware Description*, 270-702-012
- *Alcatel-Lucent 5400 Linux Control Platform User Interface Guide*, 270-702-013

- *Alcatel-Lucent 5400 Linux Control Platform Configuration Guide*, 270-702-014
- *Alcatel-Lucent 5400 Linux Control Platform Security Management Guide*, 270-702-015
- *Alcatel-Lucent 5400 Linux Control Platform Performance Management Guide*, 270-702-016
- *Alcatel-Lucent 5400 Linux Control Platform Observation Counters Dictionary*, 270-702-017
- *Alcatel-Lucent 5400 Linux Control Platform Log Management Guide*, 270-702-018
- *Alcatel-Lucent 5400 Linux Control Platform Alarm Management Guide*, 270-702-020
- *Alcatel-Lucent 5400 Linux Control Platform Alarm Dictionary*, 270-702-021
- *Alcatel-Lucent 5400 Linux Control Platform Hardware Maintenance Guide*, 270-702-030
- *Alcatel-Lucent 5400 Linux Control Platform Software Maintenance Guide*, 270-702-031
- *Alcatel-Lucent Control Platform 1800/1000/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

## Alcatel-Lucent 5450 ISC training

The following table describes related training for the Alcatel-Lucent 5450 ISC.

| Course Number | Course Title                       |
|---------------|------------------------------------|
| TIM15011W     | 5450 ISC Overview                  |
| TIM15021      | 5450 ISC OAMP                      |
| TTP21193W     | 5450 ISC Debugging Techniques      |
| TIM15001      | 5060 ICS (IP Call Server) Overview |
| IM1901        | IMS Solution Introduction          |
| TIM15010W     | 5400 LCP Overview                  |
| TIM15020      | 5400 LCP OAMP                      |

These trainings are available at the Alcatel-Lucent University Trainings website, (<https://training.alcatel-lucent.com/Saba/Web/Main>) also known as the SABA trainings website.

## Tasks

This information product describes how to perform:

- Configuration Management
- Accounting Management

---

For additional FCAPS tasks, refer to the related documentation.

### Document support

For support in using this or any other Alcatel-Lucent document, contact Alcatel-Lucent at one of the following telephone numbers:

- 1-888-582-3688 (for all United States)
- 1-630-224-2485 (for all other countries)

### Technical support

For technical support, contact your local Alcatel-Lucent customer support team. See the [Alcatel-Lucent Support web site](http://www.alcatel-lucent.com/support/) (<http://www.alcatel-lucent.com/support/>) for contact information.

### How to order

To order Alcatel-Lucent documents contact your local sales representative or use Online Customer Support (OLCS) (<https://support.alcatel-lucent.com>).

### How to comment

Note to reviewers: The following "How to comment" text will appear in the final document when it is published. However, the feedback method described below is for use only on final documents. Please send your review comments to the author using the process you were given when you received this draft document.

To comment on this document, go to the [Online Comment Form](http://infodoc.alcatel-lucent.com/comments/) (<http://infodoc.alcatel-lucent.com/comments/>) or e-mail your comments to the [Comments Hotline](mailto:Comments Hotline (comments@alcatel-lucent.com)) ([comments@alcatel-lucent.com](mailto:comments@alcatel-lucent.com)).

# Part I: Provisioning task flows

## Overview

### Purpose

This part of the documentation describes the provisioning task flows for the following:

- ISC
- SPDF
- Offline charging

### Contents

|   |     |
|---|-----|
| <a href="#">Chapter 1, ISC</a>              | 1-1 |
| <a href="#">Chapter 2, SPDF</a>             | 2-1 |
| <a href="#">Chapter 3, Offline charging</a> | 3-1 |



# 1 ISC

## Overview

### Purpose

This chapter provides the task flows:

- to configure the IP Session Control (ISC).
- to configure the parameters/timers related to the IMS Server and the IMS components part of the Alcatel-Lucent IP Session Control.
- to set up Alcatel-Lucent IP Session Control related services.

### Contents

| <b>IMS components</b>   | <b>1-4</b> |
|---|------------|
| IP Session Control configuration flow   | 1-5        |
| S-CSCF provisioning task flow   | 1-7        |
| I-CSCF provisioning taskflow  | 1-12       |
| P-CSCF provisioning task flow   | 1-15       |
| BGCF provisioning task flow   | 1-19       |
| IBCF provisioning task flow   | 1-23       |
| E-CSCF provisioning taskflow  | 1-25       |
| NTM provisioning task flow  | 1-27       |
| EEAS provisioning task flow   | 1-28       |
| IMS-GWF provisioning task flow  | 1-30       |
| iAGCF provisioning taskflow   | 1-33       |
| SIP Permanent Linksets provisioning taskflow                                  | 1-35       |
| Provision Diameter connection interface to support Multiple Destination FQDNs | 1-36       |

| <b>Services</b>  | <b>1-38</b> |
|--|-------------|
| To provision SIP forking   | 1-40        |
| Provisioning Task flow - To provision Early IMS Security provisioning  | 1-41        |
| Provisioning Task flow - To provision NASS-bundled authentication  | 1-43        |
| Symmetric TCP connections provisioning taskflow  | 1-45        |
| To provision inter-working of media between IPv4 and IPv6 networks   | 1-46        |
| Provisioning Task flow - To provision SIP Message Screening  | 1-47        |
| Provisioning Task flow - To provision Priority Mode  | 1-49        |
| Provision Integrated Security Gateway (iSGW)   | 1-51        |
| Provision P-CSCF support of generating ACRs for emergency calls  | 1-53        |
| Digit Analysis and Normalization Function - Provisioning Task flow   | 1-55        |
| ICSI provisioning task flow  | 1-57        |
| Provision Bearer Statistics Collection on iAGCF  | 1-59        |
| Provision the support of session and bandwidth limits per enterprise/PBX   | 1-60        |
| Provision the Signaling Firewall   | 1-62        |
| Signaling Firewall Load Balancer or Distribution Function with Single IP Address Exposed for the Gm Interface to End Users - Provisioning Taskflow | 1-64        |
| Cx Enhancement to support SIP Digest per 3GPP R8 - Provisioning task flow  | 1-66        |
| Provisioning Cx Enhancement per 3GPP R7 and R8   | 1-68        |
| Provision Common Announcement Module (CANM) task flow  | 1-69        |
| BGCF support for Digit Manipulation provisioning task flow   | 1-73        |
| Provision iAGCF support of Network Traffic Management (NTM)  | 1-75        |
| CMCC Emergency Service and P-CSCF SIP Header Manipulation provisioning task flow   | 1-78        |
| Support sending offline charging data to the CCF provisioned to the CTS - Provisioning task flow   | 1-80        |
| Limit for TCP Connections - Provisioning   | 1-82        |
| Enhancement of Rx and Gq' interfaces - Provisioning  | 1-83        |
| Allow SIPS-URI on Gm and Mw Interface - Provisioning   | 1-84        |
| IMUX provisioning task flow  | 1-88        |
| Provisioning Support of the NENA V5 SIP Interface to LRF and EATF for SRVCC  | 1-92        |
| Provisioning - Support MSRP Peak Data Rate to Enhance User Experience  | 1-94        |
| Provisioning - iAGCF Support of a Large Number of Residential Gateways   | 1-96        |

|   |       |
|---|-------|
| Provisioning the border access capability for H.248 interface   | 1-100 |
| Access border for IMS or Pre-IMS core provisioning task flow  | 1-104 |
| Provisioning Task flow - To provision S-CSCF Assisted Relocation Procedure for Geo-Redundancy Enhancement | 1-118 |
| Provisioning Task flow - To provision iAGCF Line OOS and CPC Display functionalities                      | 1-119 |
| To provision ATCF support   | 1-121 |
| Provisioning Task flow - To provision SIP heartbeat after failure to reach a network element              | 1-123 |
| Provisioning task flow - To provision primary and alternate SLF destination for geo-redundancy support    | 1-125 |
| Provisioning Task flow - To support new versions of IMS charging SPEC 3GPP 32.260                         | 1-127 |

# IMS components

## Overview

### Purpose

This section describes the provisioning task flows for the various IMS components.

### Contents

|   |      |
|---|------|
| IP Session Control configuration flow   | 1-5  |
| S-CSCF provisioning task flow   | 1-7  |
| I-CSCF provisioning taskflow  | 1-12 |
| P-CSCF provisioning task flow   | 1-15 |
| BGCF provisioning task flow   | 1-19 |
| IBCF provisioning task flow   | 1-23 |
| NTM provisioning task flow  | 1-27 |
| EEAS provisioning task flow   | 1-28 |
| IMS-GWF provisioning task flow  | 1-30 |
| iAGCF provisioning taskflow   | 1-33 |
| SIP Permanent Linksets provisioning taskflow                                  | 1-35 |
| Provision Diameter connection interface to support Multiple Destination FQDNs | 1-36 |

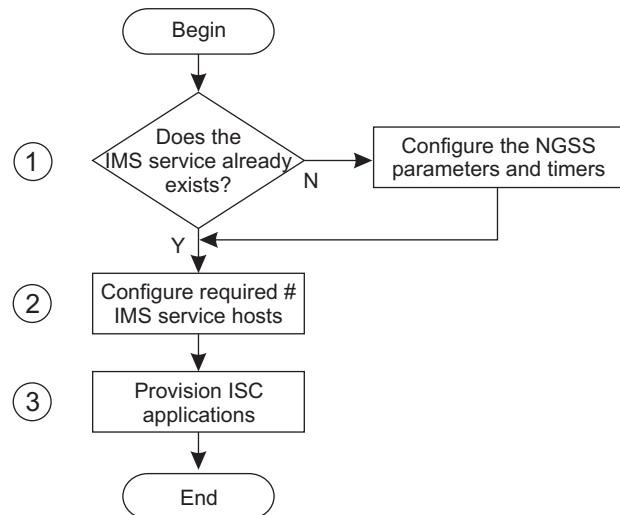
# IP Session Control configuration flow

## Purpose

This topic provides the tasks flow to create the IP Session Control (ISC) application.

## Flow diagram

The flow diagram:



## Configuration process

Perform the following steps to provision the ISC:

- 1 Configure the parameters and timers that are related to the hosts providing IMS Services (NGSS Device Servers).

| If...  | then...   |
|--|---|
| this is the first board to provision (no IMS server already exists), | refer to “To provision NGSS Server parameters” (p. 10-9). |
| an IMS server already exists,  | go to <a href="#">Stage 2</a> .                           |

- 2 Configure the required number host that must provide the IMS Service.

Refer to: “To provision an IMS Service association” (p. 10-20).

- 3** Provision the IMS applications that should run on the configured IMS service hosts.

| If you want to provision...                              | refer to...                                  |
|--|--|
| a Breakout Gateway Control Function (BGCF),              | “BGCF provisioning” (p. 4-132)               |
| a Proxy Call Session Control Function (P-CSCF),          | “P-CSCF provisioning” (p. 4-61)              |
| an Interrogating Call Session Control Function (I-CSCF), | “I-CSCF provisioning” (p. 4-44)              |
| a Serving Call Session Control Function (S-CSCF),        | “S-CSCF provisioning” (p. 4-5)               |
| an Emergency Call Session Control Function (E-CSCF),     | “E-CSCF provisioning taskflow” (p. 1-25)     |
| an E.164 Expansion Application Server (EEAS)             | “EEAS provisioning task flow” (p. 1-28)      |
| an Interconnection Border Control Function (IBCF).       | “IBCF provisioning task flow” (p. 1-23)      |
| an ACR Buffering Function (ABF)                          | “Provision ACR buffering function” (p. 8-20) |

| If you want to provision...                              | refer to...                               |
|--|---|
| a Proxy Call Session Control Function (P-CSCF),          | “P-CSCF provisioning task flow” (p. 1-15) |
| an Interrogating Call Session Control Function (I-CSCF), | “I-CSCF provisioning taskflow” (p. 1-12)  |
| a Serving Call Session Control Function (S-CSCF),        | “S-CSCF provisioning task flow” (p. 1-7)  |

# S-CSCF provisioning task flow

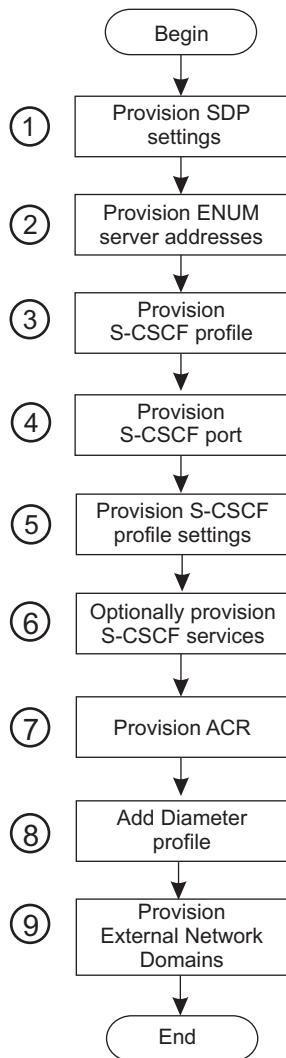
## Purpose

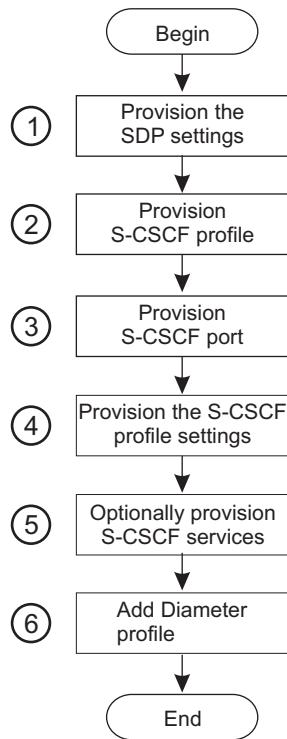
This topic provides the provisioning task flow that has to be followed to provision an S-CSCF.

## Before you begin

Observe the following:

- Using the Provisioning GUI **System View**, verify if a redundant pair of hosts have already been associated with the IMS service.
- The host pair must have enough processing capacity available for the new SIPia port.

**Provisioning task flow diagram**



## S-CSCF provisioning tasks

Perform the following steps to provision an S-CSCF:

- 1 When Local/Network policy checking have to be performed, provision SDP media to specify codecs, component policies, and subscription profiles, containing bandwidth settings and the associated parameters. These values are used to configure the S-CSCF profile.

Refer to: “[To provision SDP media](#)” (p. 4-6)

Provision an SDP profile that contains the policy of the local network and the bandwidth definition per codec. These values are used to configure the S-CSCF profile.

Refer to: “[To provision a Session Description Protocol Profile](#)” (p. 4-62)

- 2 Provision ENUM Server Addresses for I-CSCF routing.

Refer to: “[To provision ENUM server addresses](#)” (p. 10-49)

- 3 Provision an S-CSCF profile that contains the configuration that is used by the S-CSCF port.

Refer to: “[To provision an S-CSCF profile](#)” (p. 4-15)

- 
- 4 When S-CSCF capability sets are supported (returned by the HSS), provision the capability set S-CSCF of each individual S-CSCF server.

Refer to: “[To provision the S-CSCF Capability List](#)” (p. 4-53)

- 
- 5 Provision an S-CSCF application.

Provision the following parameters:

| Parameter    | Value   |
|--------------|---|
| Port Type    | Select <b>SCSF PORT</b> .   |
| Port Name    | Enter <b>sccs-<i>yyyy</i></b> .<br>Where <i>yyyy</i> is an additional identifier for the port. The recommended value for <i>yyyy</i> is <b>stdn</b> . |
| Port Profile | Select an S-CSCF profile.   |

For other parameters, retain the default values (recommended) or use a value that is required for your network.

Refer to: “[To provision a SIPia port](#)” (p. 10-40).

- 
- 6 If required, provision one or more of the following S-CSCF-specific services:

- If an emergency routing number needs to be provisioned to route the call to the emergency center associated with the geographic area of the call originator, refer to “[To provision Emergency Session Routing Method](#)” (p. 4-26).
- If the S-CSCF supports that the Application Servers originate SIP sessions using a PSI, refer to “[To provision a S-CSCF PSI URI table](#)” (p. 4-31)

- 
- 7 If the S-CSCF must generate charging data, provision ACR.

Refer to “[Provision ACR task flow](#)” (p. 3-3).

- 
- 8 Provision the Diameter interface, refer to “[To provision a Diameter profile](#)” (p. 10-23).

- 
- 9 If inter-network IMS sessions are allowed, provision the External Network Domains.

If required, provision the IBCF.

---

Refer to “[To provision an External Domain Routing table](#)” (p. 10-99)

# I-CSCF provisioning taskflow

## Purpose

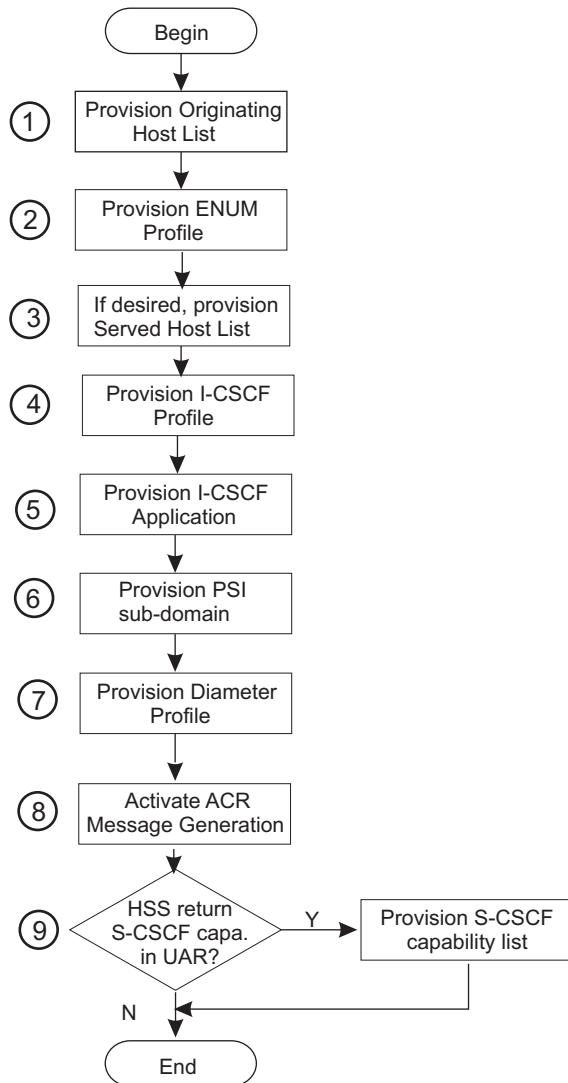
This topic provides the provisioning taskflow that should be followed to provision an I-CSCF.

## Before you begin

Observe the following:

- Using the FS GUI **System View**, a redundant pair of hosts must already have been associated with the IMS service.
- The host pair must still have enough processing capacity available for this new SIPia port.

## Provisioning taskflow diagram



## I-CSCF provisioning tasks

Perform the following steps to provision an I-CSCF on the LCP:

- 1 Provision the Originating Host List. Refer to “[To provision an Originating Hosts list](#)” ([p. 10-64](#))
- 2 Provision the ENUM profile. Refer to “[To provision the ENUM profile](#)” ([p. 10-57](#)).  
.....
- 3 Provision a I-CSCF profile that contains the configuration to be used by the I-CSCF port.  
.....

Refer to: “[To provision ICSCF Profile](#)” (p. 4-45).

- 
- 4** Provision an I-CSCF application.

Provision the following parameters:

| Parameter    | Value  |
|--------------|--|
| Port Type    | Select <b>ICSF PORT</b> .  |
| Port Name    | Enter <b>icsf-&lt;yyyy&gt;</b> .<br>Where <i>yyyy</i> is an additional identifier for the port. The recommended value for <i>yyyy</i> is <b>stdn</b> . |
| Port Profile | Select an I-CSCF profile.  |

For other parameters, retain the default values (recommended) or use a value that is required for your network.

Refer to: “[To provision a SIPia port](#)” (p. 10-40).

**Additional Information:** For information about the parameters, refer to *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

- 
- 5** If desired, provision the PSI sub-domain.

Refer to: “[To create a PSI sub-domain list](#)” (p. 4-57)

- 
- 6** Provision a Diameter profile.

Refer to “[To provision a Diameter profile](#)” (p. 10-23).

- 
- 7** If the I-CSCF must generate charging data, provision ACR.

Refer to “[Provision ACR task flow](#)” (p. 3-3).

- 
- 8** If the HSS indicates in a UAR message to the I-CSCF that it should select an S-CSCF using the Server Capability list, refer to “[To provision the S-Cscf Capability List](#)” (p. 4-53).

# P-CSCF provisioning task flow

## Purpose

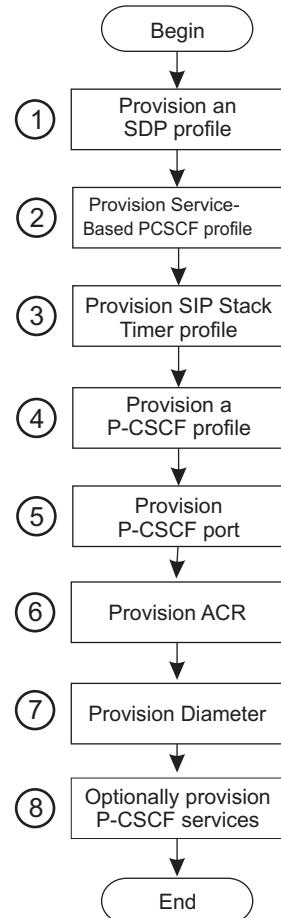
This topic provides the provisioning task flow that should be followed to provision a P-CSCF.

## Before you begin

Observe the following:

- Using the FS GUI **System View**, a redundant pair of hosts must already have been associated with the IMS service.
- The host pair must still have enough processing capacity available for this new SIP port.

## Provisioning task flow diagram



## P-CSCF provisioning tasks

Perform the following steps to provision a P-CSCF:

- 1 Provision an SDP profile that contains the policy of the local network and the bandwidth definition per codec that will be used to configure the P-CSCF profile.

Refer to: “[To provision a Session Description Protocol Profile](#)” (p. 4-62).

- 2 Optionally provision a Service-Based PCSCF profile to specify signaling compression and enforced access. It is possible to share a Service-Based PCSCF profile among multiple P-CSCF profiles.

Refer to: “[To provision Service-Based PCSCF Profile](#)” (p. 4-69).

*Note:* Provision a P-CSCF profile to enable the support of two network interfaces for SIP communication.

- 3 Optionally provision a SIP Stack Timer profile. Multiple P-CSCF profile can reference any of the defined SIP Stack Timer profiles.

Refer to “[To provision SIP Stack Timer Profile](#)” (p. 4-74).

- 4 Provision a P-CSCF profile that contains the configuration that will be used by the P-CSCF port.

Refer to: “[To provision PCSCF profile](#)” (p. 4-77).

- 5 Provision a P-CSCF application/SIPia port.

Provision the following parameters:

| Parameter    | Value  |
|--------------|--|
| Port Type    | Select <b>PCSF PORT</b> .  |
| Port Name    | Enter <b>pcsf-&lt;yyyy&gt;</b> .<br>Where <i>yyyy</i> is an additional identifier for the port. The recommended value for <i>yyyy</i> is <b>stdn</b> . |
| Port Profile | Select a P-CSCF profile.   |

| Parameter                     | Value  |
|-------------------------------|--|
| <b>Enable Two NIs for SIP</b> | Select the check box to enable two network interfaces.<br><br><i>Note:</i> This field is available for provisioning for P-CSCF port types only.  |
| <b>NTM Control Table</b>      | An update of this field in a P-CSCF will be applied across all blades that have the same port name and port type.<br><br><i>Note:</i> <ul style="list-style-type: none"> <li>This parameter is unnecessary for supporting two network interfaces for SIP communication.</li> <li>An NTM table needs to be created before assigning it to a SIPia port.</li> <li>The table ID zero means that NTM is disabled.</li> </ul> |

*Note:* To enable the support of 2 network interfaces for SIP communication on an existing P-CSCF, the P-CSCF must be deleted from every IMS service and completely removed before enabling the **Enable Two NIs for SIP** parameter and re-configuring the P-CSCF.

For other parameters, retain the default values (recommended) or use a value that is required for your network.

Refer to: “[To provision a SIPia port](#)” (p. 10-40).

**Additional information:** For information about the parameters, refer to *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

- 
- 6 If the P-CSCF must generate charging data, provision ACR.

Refer to “[Provision ACR task flow](#)” (p. 3-3).

---

- 7 Provision Diameter interface.

Refer to “[To provision a Diameter profile](#)” (p. 10-23).

- 
- 8 Optionally provision one or more of the following P-CSCF specific services:
- If the SIP header reduction service should be activated between the P-CSCF and the UE, refer to “[To activate the SIP header reduction](#)” (p. 4-101).
  - If after a successful registration, *Service Route Header* should be inserted in the 200 OK message, refer to “[To activate Service Route header](#)” (p. 4-102).
  - If SIP compression should be enabled between the P-CSCF and the UE, refer to “[To provision SIP compression](#)” (p. 4-106).
  - If secure signaling messages must be exchanged between the P-CSCF and the UE, refer to “[To provision IMS Signaling security](#)” (p. 4-108).
  - If Service Based Local Policy (SBLP) should be provisioned, refer to “[To provision the Service Based Local Policy Profile](#)” (p. 4-111).

# BGCF provisioning task flow

## Purpose

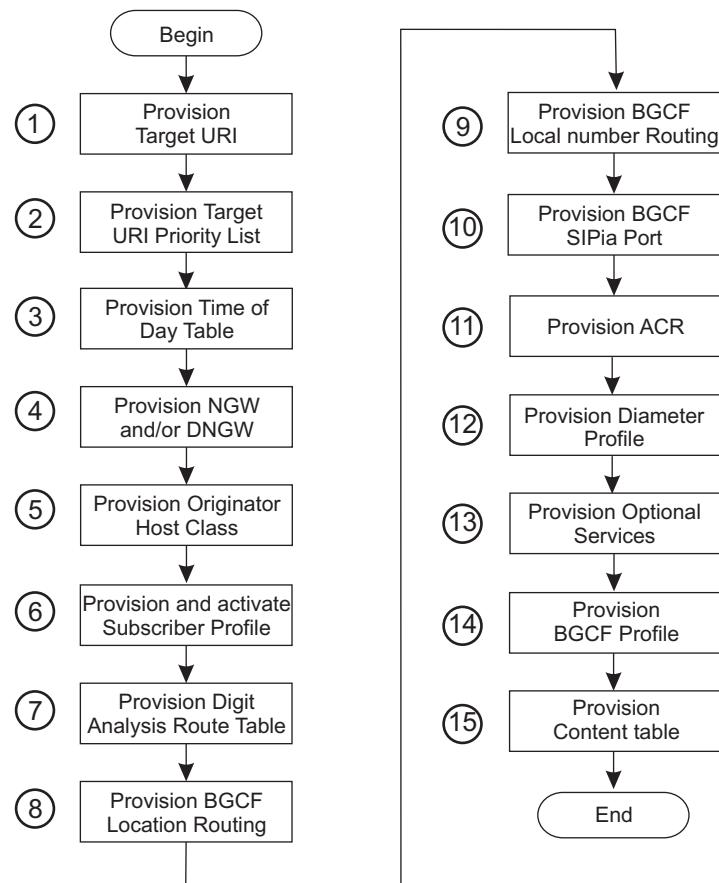
This provisioning task flow provides the steps that must be followed to provision a BGCF.

## Before you begin

Observe the following:

- Using the FS GUI **System View**, a redundant pair of hosts must be associated with the IMS service.
- The host pair must still have enough processing capacity available for this new SIPia port.

## Provisioning task flow diagram



## BGCF provisioning tasks

Perform the following steps to provision a BGCF:

- 1 Provision target Uniform Resource Identifiers (URIs) that is used to determine the next hop of the received message.  
See: “[To provision BGCF URI Id](#)” (p. 4-133)
- 2 Define a URI target list with a priority list that is used to populate the next hop list during BGCF routing.  
See: “[To provision BGCF Target List](#)” (p. 4-138)
- 3 If the Time of Day Routing is desired a Time of Day table must be populated.  
See: “[To provision BGCF Time Of Day](#)” (p. 4-148)
- 4 If required, a Network Gateway table or a Default Network Gateway table must be provisioned.  
See: “[To provision BGCF Network Gateway](#)” (p. 4-152)  
See: “[To provision BGCF Default Network Gateway](#)” (p. 4-156)
- 5 To employ Originating Host Class Profile routing functionality, a profile must be created and activated.  
See: “[To provision Originating Host Class Profile routing for BGCF](#)” (p. 4-160)
- 6 To employ subscriber profile routing functionality, a profile must be created and activated.  
See: “[To provision Subscriber Profile routing for BGCF](#)” (p. 4-163)
- 7 Provision digit match strings that is used for digit analysis of the BGCF routing.  
See: “[To provision BGCF DA Route Table](#)” (p. 4-172)
- 8 To provision the BGCF location-based routing capability, See: “[To provision BGCF local number routing](#)” (p. 4-181)

- 9 To provision the BGCF local number-based routing capability, See: “[To provision BGCF local number routing](#)” (p. 4-181)

- 10 Provision a BGCF application.

Provision the following parameters:

| Parameter    | Value  |
|--------------|--|
| Port Type    | Select <b>BGCF PORT</b> .  |
| Port Name    | Enter <b>bgcf-&lt;yyyy&gt;</b> .<br>Where <i>yyyy</i> is an additional identifier for the port. The recommended value for <i>yyyy</i> is <b>stdn</b> . |
| Port Profile | Select a BGCF profile.   |

For other parameters, retain the default values (recommended) or use a value that is required for your network.

See: “[To provision a SIPia port](#)” (p. 10-40).

**Additional information:** For information about the parameters, see *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

- 11 If the BGCF must generate charging data, provision ACR.

See “[Provision ACR task flow](#)” (p. 3-3).

- 12 Provision Diameter profile.

See: “[To provision a Diameter profile](#)” (p. 10-23).

- 13 To support the routing of SIP sessions to destinations outside of the IMS home domain, an External Domain Routing table has to be provisioned.

See: “[To provision an External Domain Routing table](#)” (p. 10-99)

Note: if an IBCF is used, this has to be provisioned as well.

- 14 Provision a BGCF profile and the corresponding digit analysis data that is used to match the BGCF Profile ID from the incoming SIP message.

See: “To provision BGCF Profile” (p. 4-142)

---

- 15 Provision the BGCF SIP content type table if different routing must be performed based on the context type of the SIP INVITE message (for example for SMS, USSD or IM messages).

See: “To provision BGCF SIP content type” (p. 4-177)

# IBCF provisioning task flow

## Purpose

This topic provides the tasks that must be carried out to provision an Interconnection Border Control Function (IBCF).

## Before you begin

Connection must be available between the LCP and foreign domains / networks

Connection must be available with the LCP DNS server and a network-level DNS server.

Published Network interfaces are required to support the desired number of services (IMS/NGSS blades) where an IBCF IMS component will be configured.

The LCP DNS server must be provisioned to recognize and forward the domain (NAPTR), network access point (SRV) and URI / URL (A) resolutions to a network-level DNS server infrastructure.

## Tasks

Carry out the following tasks:

- 
- 1 Specify global NGSS parameters.

The provisioning that is specific to the IBCF includes:

| Parameter            | Provisioning   |
|----------------------|--|
| <b>Default IBCF</b>  | The SIP URI that identifies the global IBCF; this IBCF will be used for: <ul style="list-style-type: none"><li>• All domains that are not defined in the Domain Routing table</li><li>• All non-internetworked domains for which a local IBCF is not assigned.</li></ul> |
| <b>IOI Parameter</b> | A string that identifies the Inter-Operator Identifier; this parameter is inserted by the S-CSCF or MGCF in the P-Charging-Vector header in SIP messages to identify an IMS network.   |

- 
- 2 Create an IBCF profile.

Refer to [“To provision IBCF Profile” \(p. 4-198\)](#).

---

- 3 Provision an IBCF application.

Provision the following parameters:

| Parameter           | Value  |
|---------------------|--|
| <b>Port Type</b>    | Select <b>IBCF PORT</b> .  |
| <b>Port Name</b>    | Enter <b>ibcf-&lt;xxxx&gt;</b> .<br>Where <b>xxxx</b> is an additional identifier for the port. The recommended value for <b>xxxx</b> is <b>stdn</b> . |
| <b>Port Profile</b> | Select an IBCF profile.  |

For other parameters, retain the default values (recommended) or use a value that is required for your network.

**Note:** When an IBCF SIPia port is added, two IBCF names are generated, which are ibcf-xxxx and ibgw-xxxx. The port name ibcf-xxxx is used in the home network for intra-network communication, while ibgw-xxxx is used outside of the home network for inter-network communication. This setup is required for security and THIG consideration. Also, ibcf-xxxx is associated with the default NI, while ibgw-xxxx is associated with the published NI.

Refer to: “To provision a SIPia port” (p. 10-40).

- 
- 4 If the IBCF must generate charging data, provision ACR.

Refer to “Provision ACR task flow” (p. 3-3).

# E-CSCF provisioning taskflow

## Purpose

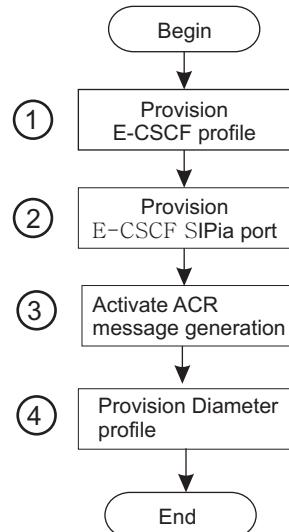
This topic provides the provisioning taskflow that should be followed to provision an E-CSCF.

## Before you begin

Observe the following:

- Using the FS GUI **System View**, a redundant pair of hosts must already have been associated with the IMS service.
- The host pair must still have enough processing capacity available for this new SIPia port.

## Provisioning taskflow diagram



## E-CSCF provisioning tasks

Perform the following steps to provision an E-CSCF:

- 1 Provision the E-CSCF Profile.

Refer to: [“To provision an E-CSCF Profile table” \(p. 4-212\)](#).

If the E-CSCF will be provisioned to support the 3GPP and TISPAN standard, define an IMS Emergency Service Identifier.

Refer to: [“To provision IMS Emergency Service Identifier” \(p. 4-208\)](#).

---

**2** Provision an E-CSCF application.

Provision the following parameters:

| Parameter    | Value   |
|--------------|---|
| Port Type    | Select <b>ECSF PORT</b> .   |
| Port Name    | Enter <b>ecsfc-&lt;yyyy&gt;</b> .<br>Where <i>yyyy</i> is an additional identifier for the port. The recommended value for <i>yyyy</i> is <b>stdn</b> . |
| Port Profile | Select an E-CSCF profile.   |

For other parameters, retain the default values (recommended) or use a value that is required for your network.

Refer to: “To provision a SIPia port” (p. 10-40).

---

**3** If the E-CSCF must generate charging data, provision ACR.

Refer to: “Provision ACR task flow” (p. 3-3).

---

**4** **Note:** This step is needed for ECSF-HSS ESRM only.

Provision Diameter profile.

Refer to “To provision a Diameter profile” (p. 10-23).

# NTM provisioning task flow

## Purpose

This topic provides the provisioning task flow to provision NTM.

## Before you begin

Observe the following:

- Using the FS GUI **System View**, a redundant pair of hosts must already have been associated with the IMS service.
- The host pair must still have enough processing capacity available for this new SIPia port.

## Related Information

NTM table needs to be created before assigning to SIPia port. Also, the table ID zero means NTM is disabled.

## NTM provisioning tasks

Perform the following steps:

- 
- 1 Provision the NTM Control table.

Refer to: [“To provision an NTM Control table” \(p. 4-222\)](#)

---

- 2 Provision an NTM Exemption table.

Refer to: [“To provision an NTM Exemption table ” \(p. 4-226\)](#)

# EEAS provisioning task flow

## Purpose

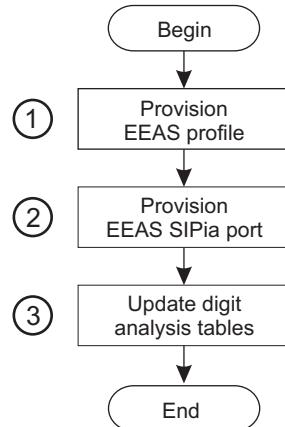
This topic provides the provisioning task flow to provision an E.164 Expansion Application Server (EEAS).

## Before you begin

Observe the following:

- Using the Provisioning GUI **System View**, a redundant pair of hosts must already have been associated with the IMS service.
- The host pair must still have enough processing capacity available for this new SIPia port.
- An HSS is provisioned with initial Filter Criteria (iFC) for IMS originating sessions and for IMS terminating sessions.

## Provisioning taskflow diagram



## EEAS provisioning tasks

Perform the following steps:

- 
- 1 Provision the EEAS Profile.

Refer to: “To provision an E.164 Expansion AS profile” (p. 4-238)

---

- 2 Provision an EEAS application.

Provision the following parameters:

| Parameter           | Value   |
|---------------------|---|
| <b>Port Type</b>    | Select <b>EEAS PORT</b> .   |
| <b>Port Name</b>    | Enter <b>eeas-&lt;yyyy &gt;</b> .<br>Where <b>yyyy</b> is an additional identifier for the port. The recommended value for <b>yyyy</b> is <b>stdn</b> . |
| <b>Port Profile</b> | Select an EEAS profile.   |

For other parameters, retain the default values (recommended) or use a value that is required for your network.

Refer to: “[To provision a SIPia port](#)” (p. 10-40).

### 3 Update digit analysis tables

If digits are added in front of the called number via the **Prefix to Prepend** field of the EEAS Profile, then very likely the digit tables of other network elements need to be updated as well.

For example, suppose you want to force a call through the PSTN network using the EEAS. Suppose the **Prefix to Prepend** digits are **99**.

Then the BGCF must recognize the addresses with the provisioned “Prefix to Prepend”. These addresses must be routed towards the appropriate MGCF.

Suppose the BGCF has an entry for a subscriber with the **Digit String** = **+1630979&**. This would terminate to an I-CSCF (normal IMS termination), but with an additional entry in the same table with **Digit String** = **+991630979&** the call terminates to an MGCF.

However, before the MGCF routes the call to the PSTN, the prefixed digits must be removed. So, an entry in the MGCF digit table must be made to take care of that: **99630&** translates to **630&**.

# IMS-GWF provisioning task flow

## Purpose

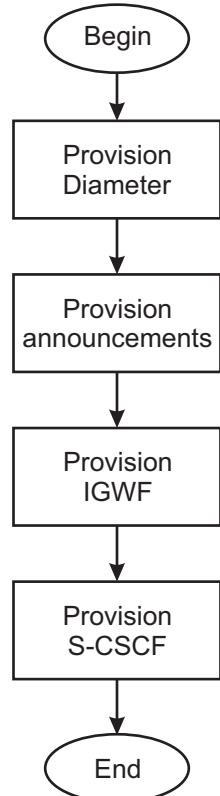
This topic provides the task flow for configuring an IMS Gateway Function (IMS-GWF). The IMS-GWF acts as an interface to an Online Charging System.

## Assumptions

This task flow assumes that the following tasks have been completed:

- OCS installation and OCS basic configuration is completed.
- OCS is physical connected to the IMS-GWF.

## Task flow



## Task flow stages

Perform the following stages to provision online charging:

- 1 Verify that a network interface for the Diameter Ro interface is configured on the IMS service.
  1. At the Provisioning GUI, click **System View**
  2. Select **Services** → **IMS**
  3. Select the IMS service you want to configure the IMS-GWF on.
  4. Right-click and select **Modify**.

The External Floating IP Address Assignments section must have an NI Type = Ro/Diameter.

- 2 Define a Diameter application ID for the Ro interface.

The default value for the Diameter application ID for the Ro interface is 4.

**Reference:** Refer to “To modify Diameter application IDs” (p. 10-31).

- 3 Add a Diameter profile for the Ro interface. The Diameter profile has a Diameter Connection Interface for Ro.

**Reference:** Refer to “To provision a Diameter profile” (p. 10-23).

- 4 Import an MRF Announcement Data table. You cannot add or modify this table.

**Reference:** Refer to “To provision MRF Announcement Data table” (p. 4-247).

- 5 Provision MRF Announcement Interface profile.

**Reference:** Refer to “To provision MRF Announcement Interface profile” (p. 4-245).

- 6 Configure the Online Charging Trigger Data.

**Reference:** Refer to “To provision Online Charging Trigger Data table” (p. 4-242).

- 7 Provision an IGWF profile

**Reference:** Refer to “[To provision IGWF profile](#)” (p. 4-250).

- 
- 8 Provision an IGWF SIPia port.

Provision the following parameters:

| Parameter    | Value  |
|--------------|--|
| Port Type    | Select <b>IGWF PORT</b> .  |
| Port Name    | Enter <b>igwf-&lt;yyyy&gt;</b> .<br>Where <b>yyyy</b> is an additional identifier for the port. The recommended value for <b>yyyy</b> is <b>stdn</b> . |
| Port Profile | Select a IGWF profile  |

For other parameters, retain the default values (recommended) or use a value that is required for your network.

**Reference:** Refer to “[To provision a SIPia port](#)” (p. 10-40).

- 
- 9 Unlock the IGWF SIPia port.

- 
- 10 Provision an online charging profile.

**Reference:** Refer to “[To provision an Online Charging Profile table](#)” (p. 9-3).

- 
- 11 Provision the S-CSCF profile for online charging.

**Reference:** Refer to “[Provision S-CSCF profile for online charging](#)” (p. 9-7).

# iAGCF provisioning taskflow

## Purpose

This topic provides the provisioning taskflow that should be followed to provision an iAGCF for:

- an ICS Solution, and
- a Distributed IMS Solution.

## iAGCF provisioning tasks

Perform the following steps to provision an iAGCF:

1 Provision base configuration. Refer to “[To execute the base configuration](#)” (p. 10-6).

2 Start and verify the FSDB. Refer to “[To start and verify the FSDB](#)” (p. 10-8).

3

| For the:     | Add the iAGCF switch type comprising of:                |
|--------------|---|
| IMS Solution | 5420 CTS and iAGCF to the OMC-P management view.        |
| ICS Solution | 5420 CTS, iHSS, and iAGCF to the OMC-P management view. |

Refer to topic “Add Switch to OMC-P” in *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420.

4 Provision tables with customer data for:

| Sequence | Procedure   | Provisioning tool |
|----------|---|-------------------|
| 1        | Add an emergency service identifier. Refer to “ <a href="#">To provision IMS Emergency Service Identifier</a> ” (p. 4-208).<br><br>Note: At least one entry must exist in the Emergency Identifiers List in order to create an iAGCF profile. | FS GUI            |
| 2        | Provision the iAGCF Profile.  | OMC-P*            |

| Sequence | Procedure  | Provisioning tool |
|----------|--|-------------------|
| 3        | Provision the iAGCF Digit Map.   | OMC-P*            |
| 4        | Provision the iAGCF Gateway Variant.   | OMC-P*            |
| 5        | Add a new SIPia component (iAGCF) in the SIPia Port Configuration window. Refer to “ <a href="#">To provision a SIPia port</a> ” (p. 10-40). | FS GUI            |
| 6        | Add PRSET type in the SCSCF Profile. Refer to “ <a href="#">To provision an S-CSCF profile</a> ” (p. 4-15).                                  | FS GUI            |
| 7        | Provision the iAGCF Gateway.   | OMC-P*            |

**Notes:**

1. In case the Gateway registration and iAGCF subscriber provisioning data become inconsistent between the H.248, SIP and FSDB, select an LCP Switch in the OMC-P, click **Configuration → AGCF Specific Configuration → AGCF Gateway Table → Gateways**, right-click a gateway entry, and select **Send Refresh to GW....** The IMS service assigned to the gateway performs a registry audit of the AGCF data. The AGCF H.248 will send the Registration Status to SIP immediately and starts H.248 Audit of the Gateway.
2. The value of the iAGCF Gateway Domain depends on the NGSS Parameters **Enable multiple home domains** setting. If this check box is not selected, the iAGCF gateway domain must be the NGSS Parameter default home domain value. If it is selected, iAGCF gateway domain value must be listed in the Home Domains table of the P-NAPTR records. Note: Before changing or deleting the NGSS Parameters default domain or multiple home domains, delete all AGCF Gateways using that domain.

\*For provisioning procedures, refer to *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420.

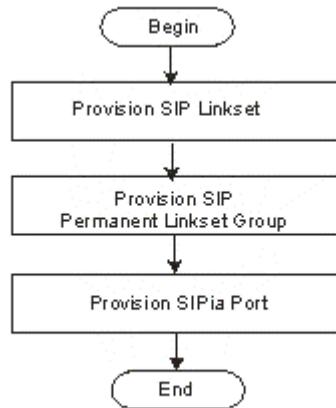
**Note:** When the OMC-P is present, only the OMC-P should be used for iAGCF provisioning.

# SIP Permanent Linksets provisioning taskflow

## Purpose

This topic provides the task flow that should be followed to provision SIP Permanent Linksets.

## Provisioning SIP Permanent Linksets taskflow



## Provisioning SIP Permanent Linksets

Perform the following steps to provision SIP Permanent Linksets:

- 1 Provision a SIP Linkset.

Refer to “[To provision an SIP Linkset](#)” (p. 4-264).

- 2 Provision a SIP Permanent LinkSet Group.

Refer to “[To provision an SIP Permanent Linkset Group](#)” (p. 4-269).

- 3 Provision a SIPia Port.

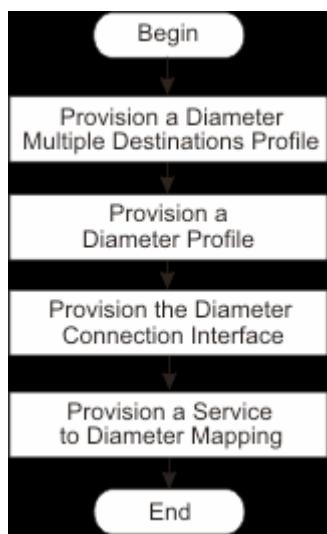
Refer to “[To provision a SIPia port](#)” (p. 10-40).

# Provision Diameter connection interface to support Multiple Destination FQDNs

## Purpose

This topic provides the procedure that should be followed to provision Diameter connection interface to support Multiple Destination FQDNs.

## Provisioning task flow diagram



## Provision Diameter connection interface to support Multiple Destination FQDNs

Perform the following steps:

- 1 Provision a Diameter Multiple Destinations Profile.

Refer to “[To provision a Diameter Multiple Destination Profile](#)” (p. 4-278).

- 2 Provision a Diameter Profile.

Refer to “[To provision a Diameter profile](#)” (p. 10-23).

- 3 Provision the Diameter Connection Interface.

Provision the Application Type “Cx” or “Sh” and select the Diameter Multiple Destinations Profile ID. Refer to “[To provision a Diameter profile](#)” (p. 10-23).

---

**4 Provision Service to Diameter Mapping.**

Provision the IMS service to the Diameter Profile. Refer to “[To provision a Service to Diameter mapping](#)” (p. 10-32).

# Services

## Overview

### Purpose

This section describes the provisioning task flows that are required to set up Alcatel-Lucent IP Session Control related services.

### Contents

|  |      |
|--|------|
| To provision SIP forking   | 1-40 |
| Provisioning Task flow - To provision Early IMS Security provisioning  | 1-41 |
| Provisioning Task flow - To provision NASS-bundled authentication  | 1-43 |
| Symmetric TCP connections provisioning taskflow  | 1-45 |
| To provision inter-working of media between IPv4 and IPv6 networks   | 1-46 |
| Provisioning Task flow - To provision SIP Message Screening  | 1-47 |
| Provisioning Task flow - To provision Priority Mode  | 1-49 |
| Provision Integrated Security Gateway (iSGW)   | 1-51 |
| Provision P-CSCF support of generating ACRs for emergency calls  | 1-53 |
| Digit Analysis and Normalization Function - Provisioning Task flow   | 1-55 |
| ICSI provisioning task flow  | 1-57 |
| Provision Bearer Statistics Collection on iAGCF  | 1-59 |
| Provision the support of session and bandwidth limits per enterprise/PBX   | 1-60 |
| Provision the Signaling Firewall   | 1-62 |
| Signaling Firewall Load Balancer or Distribution Function with Single IP Address Exposed for the Gm Interface to End Users - Provisioning Taskflow | 1-64 |
| Cx Enhancement to support SIP Digest per 3GPP R8 - Provisioning task flow  | 1-66 |
| Provisioning Cx Enhancement per 3GPP R7 and R8   | 1-68 |
| Provision Common Announcement Module (CANM) task flow  | 1-69 |
| BGCF support for Digit Manipulation provisioning task flow   | 1-73 |
| Provision iAGCF support of Network Traffic Management (NTM)  | 1-75 |
| CMCC Emergency Service and P-CSCF SIP Header Manipulation provisioning task flow   | 1-78 |

|   |       |
|---|-------|
| Support sending offline charging data to the CCF provisioned to the CTS - Provisioning task flow          | 1-80  |
| Limit for TCP Connections - Provisioning  | 1-82  |
| Enhancement of Rx and Gq' interfaces - Provisioning   | 1-83  |
| Allow SIPS-URI on Gm and Mw Interface - Provisioning  | 1-84  |
| IMUX provisioning task flow   | 1-88  |
| Provisioning Support of the NENA V5 SIP Interface to LRF and EATF for SRVCC                               | 1-92  |
| Provisioning - Support MSRP Peak Data Rate to Enhance User Experience                                     | 1-94  |
| Provisioning - iAGCF Support of a Large Number of Residential Gateways                                    | 1-96  |
| Provisioning the border access capability for H.248 interface   | 1-100 |
| Access border for IMS or Pre-IMS core provisioning task flow  | 1-104 |
| Provisioning Task flow - To provision S-CSCF Assisted Relocation Procedure for Geo-Redundancy Enhancement | 1-118 |
| Provisioning Task flow - To provision iAGCF Line OOS and CPC Display functionalities                      | 1-119 |
| To provision ATCF support   | 1-121 |
| Provisioning Task flow - To provision SIP heartbeat after failure to reach a network element              | 1-123 |
| Provisioning task flow - To provision primary and alternate SLF destination for geo-redundancy support    | 1-125 |
| Provisioning Task flow - To support new versions of IMS charging SPEC 3GPP 32.260                         | 1-127 |

# To provision SIP forking

## Purpose

This procedure is used to provision SIP forking.

## Steps to provision SIP forking

- 1 Verify the timer settings for the default SIP Stack timer profile (Profile Id=0) and the SIP Stack timer profile for the P-CSCF.

If required, update and create the profiles.

See “[To provision SIP Stack Timer Profile](#)” (p. 4-74).

- 2 Verify if the SIP stack timer profile for P-CSCF is assigned as the **SIP Stack Timer Profile Id** in the PCSCF Profile Attributes.

See “[To provision PCSCF profile](#)” (p. 4-77).

- 3 Provision SIP forking in the SCSCF Profile Attributes.

1. Enable **Allow Forking**
2. Provision the **Forking Answer Guard Timer**
3. Select the default handling parameters.

See “[To provision an S-CSCF profile](#)” (p. 4-15).

For more information about the parameters, refer to *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

# Provisioning Task flow - To provision Early IMS Security provisioning

## Purpose

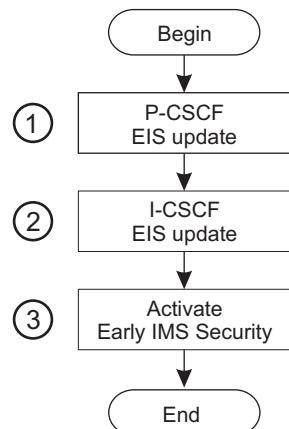
This provisioning task flow is used to provision Early IMS Security.

## Before you begin

### Points to remember

- These provisioning steps are only applicable for a Unified Subscriber Data Server (USDS) type HSS.
- The UEs intended to work for this feature need to have the IP addresses configured on the HSS.

## Provisioning task flow diagram



## Steps to provision Early IMS Security

Perform the following steps:

### 1 P-CSCF EIS update.

On the **P-CSCF Profile Attributes** screen, set the following parameters:

- Set the parameter **Preserve Via header** to **yes**.
- Set the parameter **Access Type** to **3GPP-GERAN** and set the parameter **Support TISPAN e2 Interface** to **Disabled**.

See “[P-CSCF provisioning](#)” (p. 4-61).

---

**2 I-CSCF EIS update.**

On the **I-CSCF Profile Attributes** screen, set the parameter **Register without Authorization Header** according to the following table:

| HSS type            | Register without Authorization Header   |
|---------------------|---|
| USDS HSS            | <b>Set IMPI to Zero</b>   |
| Other HSS than HSDS | <b>Challenge</b><br><i>Note:</i> Select this option if MD5 and EIS registrations are allowed on the S-CSCF<br><b>Reject</b><br><i>Note:</i> Select this option when MD5 registration is not allowed on the I-CSCF |

See “[I-CSCF provisioning](#)” (p. 4-44).

---

**3 Activate Early IMS Security.**

Activate the Early IMS Security service by selecting **Early IMS Security** on the **S-CSCF Profile Attributes** screen.

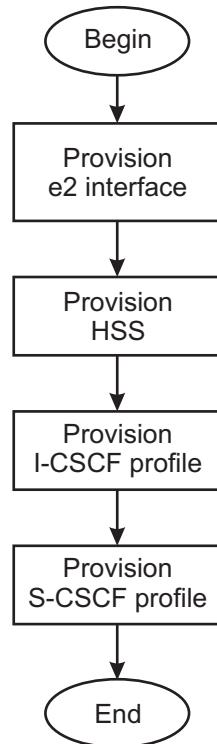
The activation specifies that the Early IMS security algorithm is used, when the right conditions are met.

# Provisioning Task flow - To provision NASS-bundled authentication

## Purpose

This provisioning task flow is used for configuring NASS-bundled authentication. NASS-bundled authentication is an authentication schema to authenticate UEs using user location. NASS-bundled authentication is defined by TISPAN.

## Provisioning task flow diagram



## Steps to provision NASS-bundled authentication

Perform the following steps to provision NASS-bundled authentication:

- 1 Provision the e2 interface between the P-CSCF and the CLF.  
See “To provision e2 interface support” (p. 4-116).
- 2 Provision authorized user locations on the HSS

Refer to the HSS documentation.

**3** Provision the I-CSCF profile.

Configure the following parameters:

| Parameter                      | Value     |
|--------------------------------|-----------|
| Register without Authorization | Challenge |

See “[To provision ICSCF Profile](#)” (p. 4-45).

**4** Provision the S-CSCF profile.

Configure the following parameters:

| Parameter    | Value   |
|--------------|---------|
| NASS Bundled | Checked |

See “[To provision an S-CSCF profile](#)” (p. 4-15).

# Symmetric TCP connections provisioning taskflow

## Overview

This topic describes the taskflow to provision symmetric TCP connections.

## Related information

For more information on the feature, see the topic “*Symmetric TCP Connections*” in the *ISC Application User Guide*.

## Task flow stages

Perform the following stages to provision symmetric TCP connections:

- 
- 1 Provision the NGSS Server parameters.

Configure the following parameters:

| Parameter  | Value            |
|--|------------------|
| Percent of Users with Simultaneous TCP Connections | 0 to 100 percent |

**Reference:** Refer to “[To provision NGSS Server parameters](#)” (p. 10-9) .

---

- 2 Provision the P-CSCF profile.

Select one of the following values for the following parameters:

| Parameter                | Value   |
|--------------------------|---|
| Symmetric TCP Connection | <ul style="list-style-type: none"><li>• Off</li><li>• Always</li><li>• FW-NAT or SIP Outbound</li></ul> |

**Reference:** Refer to “[To provision PCSCF profile](#)” (p. 4-77) .

# To provision inter-working of media between IPv4 and IPv6 networks

## Purpose

This procedure is used to provision inter-working of media between IPv4 and IPv6 networks.

## Before you begin

Inter-working of media between the IPv4 and IPv6 networks is supported only on the 5400 LCP. For LCP 1800, only IPv4 is supported.

## Steps to provision inter-working of media between IPv4 and IPv6 networks

Perform the following steps:

- 1 Set the **IMS Core IP Version for Media Interworking** parameter in the NGSS Parameters/Timers screen to either **IPv4** or **IPv6**. See “[To provision NGSS Server parameters](#)” (p. 10-9).
- 2 Set the **IPv6 Unspecified Address Format** parameter to either :: or xxx.invalid. See “[To provision the Service Based Local Policy Profile](#)” (p. 4-111).
- 3 Set the **Remote Network IP Version** parameter in the IBCF Profile Attributes to either **IPv4** or **IPv6**, for each IBCF interface. See “[To provision IBCF Profile](#)” (p. 4-198).
- 4 For inter-working IPv4 and IPv6 for iAGCF, perform the following:
  1. Enable the **Service Based Local Policy Enabled** parameter in the **AGCF Profile** screen.
  2. Select the appropriate SBLP Profile ID in the **SBLP Profile Id** parameter in the **AGCF Profile** screen.

Refer to the topic, “Provision the iAGCF Profile” in *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420.

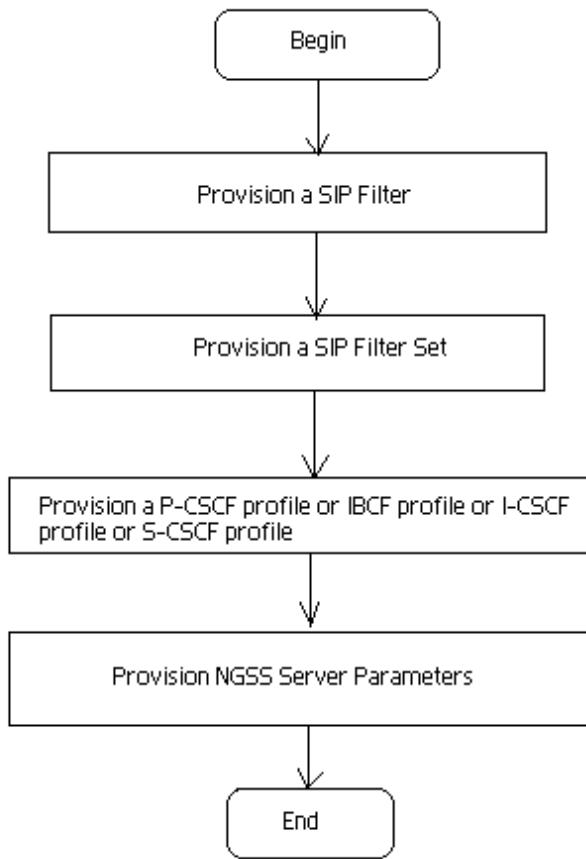
END OF STEPS

# Provisioning Task flow - To provision SIP Message Screening

## Purpose

This provisioning task flow should be followed to provision SIP Message Screening.

## Provisioning task flow diagram



## Steps to provision SIP Message Screening

Perform the following steps:

- 1 Provision an SIP Filter.

**Note:** The SIP Filter must be set to active (that is, enabled) after provisioning the SIP Filter, SIP Filter Header Rule, SIP Filter Body Rule, SIP Filter Reference Rule and SIP Filter Parameter Rule.

For more information on provisioning an SIP Filter, SIP Filter Header Rule, SIP Filter Body Rule, SIP Filter Reference Rule and SIP Filter Parameter Rule, refer “[To provision an SIP Filter](#)” (p. 5-23), “[To provision an SIP Filter Header Rule](#)” (p. 5-28), “[To provision an SIP Filter Body Rule](#)” (p. 5-36), “[To provision an SIP Filter Reference Rule](#)” (p. 5-44) and “[To provision an SIP Filter Parameter Rule](#)” (p. 5-50).

---

**2** Provision an SIP Filter Set.

See “[To provision an SIP Filter Set](#)” (p. 5-57).

---

**3** Provision a P-CSCF Profile/IBCF Profile (as desired).

Provision the SIP Filter Set parameter for the P-CSCF profile /IBCF profile /S-CSCF profile /I-CSCF Profile.

See “[To provision PCSCF profile](#)” (p. 4-77) / “[To provision IBCF Profile](#)” (p. 4-198) /“[To provision ICSCF Profile](#)” (p. 4-45) /“[To provision an S-CSCF profile](#)” (p. 4-15) .

---

**4** Provision NGSS Server Parameters.

**Note:** To activate SIP message screening functionality, you need to enable the SIP Message Screening parameter. However, enabling or disabling the SIP Message Screening parameter does not affect the provisioning of SIP Filters or SIP Filter Sets.

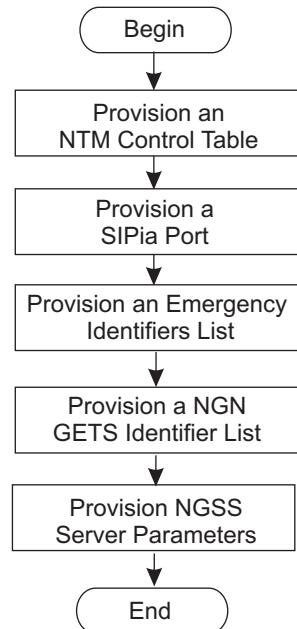
For more information on provisioning the SIP Message Screening parameter, see “[To provision NGSS Server parameters](#)” (p. 10-9).

# Provisioning Task flow - To provision Priority Mode

## Purpose

This provisioning task flow provides the steps to provision Priority Mode.

## Provisioning task flow diagram



## Steps to provision Priority Mode

Perform the following steps to provision Priority Mode.

- 1 Provision an NTM Control Table.

See “[To provision an NTM Control table](#)” (p. 4-222).

- 2 Provision a SIPia Port.

Provision the NTM Parameters.

See “[To provision a SIPia port](#)” (p. 10-40).

- 3 Provision an Emergency Identifiers List.

See “[To provision an Emergency Identifiers List](#)” (p. 5-61).

- 
- 4 Provision an NGN GETS Identifier List.

See “[To provision an NGN GETS Identifier List](#)” (p. 5-64).

---

- 5 Provision NGSS Server Parameters.

Provision the Priority Mode parameter.

See “[To provision NGSS Server parameters](#)” (p. 10-9).

# Provision Integrated Security Gateway (iSGW)

## Purpose

This topic describes the provisioning tasks that must be followed to provision the Integrated Security Gateway.

## Before you begin

For information regarding the quarantine configuration impacts, see *Section: Configuring the Integrated Security Gateway, Topic: P-CSCF Configuration* in the *Alcatel-Lucent Access Border Solution Planning and Implementation Guide*, 255-900-359R8.3.

## Procedure

The Integrated Security Gateway service provides a function to configure the Integrated Security Gateway. Each step in the procedure provides instructions to enable a function. Perform the following steps to provision the Integrated Security Gateway:

- 
- 1 Configure the Integrated Security Gateway function.
    - 1 Provision a SIP Flow Trusted Rate Limit Rule Set and a SIP Flow Untrusted Rate Limit Rule Set.  
See, “[To provision an SIP Flow Trusted/Untrusted Rate Limit Rule Set](#)” (p. 5-68).
    - 2 Provision Trusted and Untrusted entries in the Flow Source Address Policy tables.  
See, “[To provision a Flow Source Address Policy](#)” (p. 5-76).
    - 3 Provision a SIP Aggregate Trusted Rate Limit Rule Set and a SIP Aggregate Untrusted Rate Limit Rule Set.  
See, “[To provision an SIP Aggregate Trusted/Untrusted Rate Limit Rule Set](#)” (p. 5-72).
    - 4 Provision Trusted and Untrusted entries in the Aggregate Source Address Policy tables.  
See, “[To provision an Aggregate Source Address Policy](#)” (p. 5-80)
    - 5 Provision a Registration Failure Policy table.  
See, “[To provision a Registration Failure Policy](#)” (p. 5-83)
    - 6 Provision an Application Failure Policy table.  
“[To provision an Application Layer Policy](#)” (p. 5-87)
    - 7 Provision a Security Gateway profile.

- See, “[To provision a Security Gateway Profile](#)” (p. 5-90).
8. Select the configured Security Gateway profile in the **Security Gateway Profile Id** list, in the **Security Parameters** tab of the P-CSCF profile.

To apply registration suppression, provision the **Registration** group in the **General Parameters** tab of the P-CSCF profile.

See, “[To provision PCSCF profile](#)” (p. 4-77).

**Note:**

- To activate the Integrated Security Gateway function, ensure that the **Enable Two NIs for SIP** check box is selected in the **General Parameters** tab of the P-CSCF profile.
- An Integrated Security Gateway can be activated for a P-CSCF SIPia port at any time. It is recommended that the P-CSCF SIPia port be removed from service before the Security Gateway is enabled. If the Security Gateway is enabled while the P-CSCF is in-service, the Trusted Rate rules configured for the Security Gateway are not adhered to, while handling the current SIP messaging or Keep-Alive traffic. This condition can persist until users Re-register, which ensures that their Trusted status is updated in the Security Gateway.

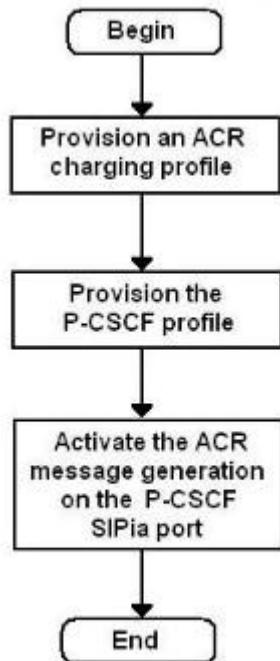
E N D O F S T E P S

# Provision P-CSCF support of generating ACRs for emergency calls

## Purpose

Follow this procedure to provision the P-CSCF support of generating ACRs for emergency calls.

## Provisioning task flow



## Provisioning steps

Perform the following steps:

- 1 Provision an ACR charging profile with the **ACR Generation For Emergency Calls** parameter selected.

Refer “[To provision an ACR Charging Profile](#)” (p. 8-5).

- 2 Provision the P-CSCF profile to support the 3GPP emergency calls. Assign the new ACR charging profile ID in the **ACR Charging Profile ID** drop-down box.

---

Refer “[Assigning an ACR Charging profile to an IMS entity](#)” (p. 8-15).

---

- 3** Activate the ACR message generation on the P-CSCF SIPia port.

Refer “[To activate an ACR message generation on a SIPia port](#)” (p. 8-3).

**E N D O F S T E P S**

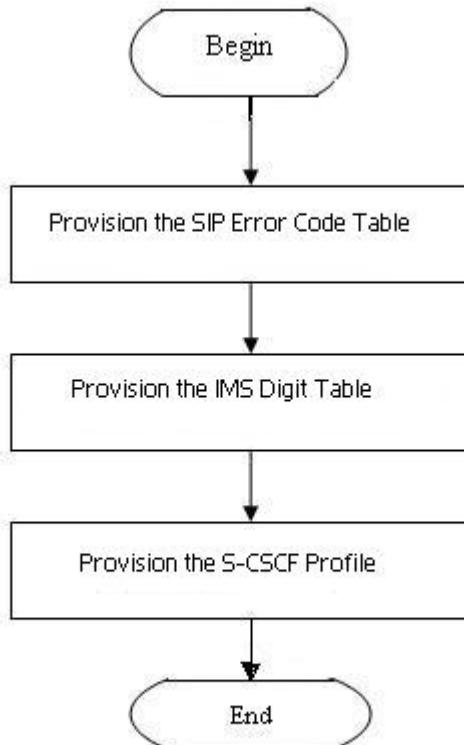
---

# Digit Analysis and Normalization Function - Provisioning Task flow

## Purpose

This topic provides the task flow for support of Digit Analysis and Normalization Function.

## Task flow



## Task flow stages

Perform the following:

- 1 Provision the SIP Error Code Table.

Refer to “[To provision a SIP Error Code table](#)” (p. 5-106)

---

2 Provision the IMS Digit Table.

Refer to “[To provision an IMS Digit Table](#)” (p. 5-110)

---

3 To provision the S-CSCF Profile to support Digit Analysis and Normalization Function  
configure the following parameters:

- Select the **Invoke DA after completion of iFC processing** check box under the **Digit Analysis** tab of the S-CSCF Profile.
- Select the appropriate value from the **Digit Table Id** drop down menu.

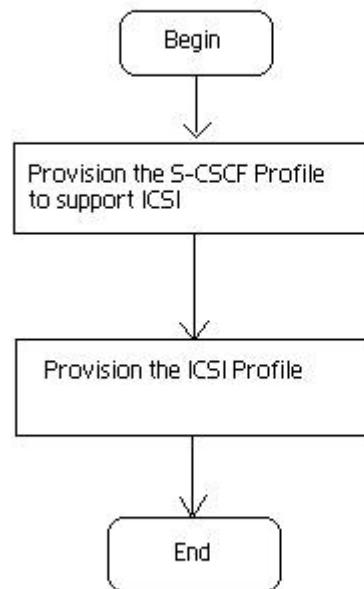
Refer to “[To provision an S-CSCF profile](#)” (p. 4-15)

# ICSI provisioning task flow

## Purpose

This topic describes the task flow that should be followed for provisioning the IMS Communication Service Identifier (ICSI).

## Provisioning task flow diagram



## ICSI provisioning

- 1 Provision the S-CSCF Profile to support ICSI.

Enable the following options on the S-CSCF Profile.

- For checking of error cases for an initial request, enable the **Only allow initial SIP requests for subscribed ICSI and compliant to policy** check box.
- For checking of error cases for a target refresh request, enable the **Only allow modification to SIP dialogs that aligns with ICSI identified at start of dialog** check box.
- To determine the disposition of handling request without P-Preferred-Service or P-Asserted-Service for an ICSI subscriber, enable the **Search initial SIP requests without ICSI for presence of ICSI attributes** check box.

For more information on S-CSCF provisioning to support ICSI, refer to “[To provision an S-CSCF profile](#)” (p. 4-15).

---

**2 Provision the ICSI Profile.**

For more information on ICSI profile provisioning, refer to “[To provision an ICSI profile](#)” (p. 5-117).

# Provision Bearer Statistics Collection on iAGCF

## Purpose

This procedure is used to provision Bearer Statistics Collection on iAGCF.

## Procedure

Perform the following steps:

- 
- 1 Configure the following parameters in the NGSS Server Parameters/Timer screen:

- **SPDF Node-functionality**
- **AGCF Node-functionality**

Refer to “[To provision NGSS Server parameters](#)” (p. 10-9).

---

- 2 Select the **ACR Messages Generation** check box in the SIPia Port Configuration screen.

Refer to “[To provision a SIPia port](#)” (p. 10-40).

---

- 3 Select the appropriate value from the **ACR Charging Profile ID** drop down menu in the AGCF Profile Screen.

Refer to the topic, “Provision the iAGCF Profile” in *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420.

---

- 4 Select the **Request Bearer Statistics** check box in the AGCF Gateway Variant Screen.

**Note:** This field controls whether or not to include Audit{Statistics} in Subtract command to request the Bearer Statistics from the AGW variant.

For provisioning procedures, refer to *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420.

END OF STEPS

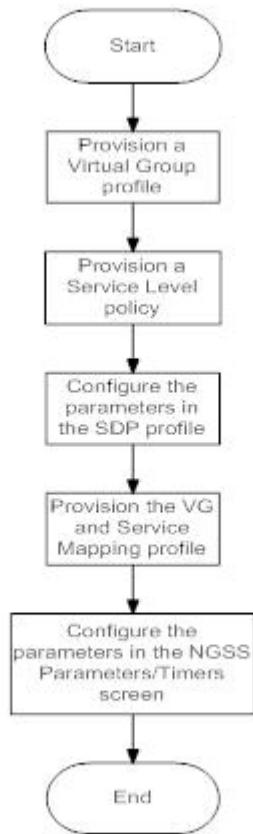
---

# Provision the support of session and bandwidth limits per enterprise/PBX

## Purpose

This topic provides the provisioning task flow that should be followed to provision the support of session and bandwidth limits per enterprise/PBX.

## Provisioning task flow



## Provisioning procedure

Perform the following steps to provision the support of session and bandwidth limits per enterprise/PBX:

- 1 Provision a Virtual Group profile.

Refer, “[To provision a Virtual Group profile](#)” (p. 5-125).

---

**2** Provision a Service Level policy.

Refer, “[To provision a Service Level Policy](#)” (p. 5-129).

---

**3** Configure the parameters within the **VG Session and BW Control** section of the SDP profile.

Refer, “[To provision a Session Description Protocol Profile](#)” (p. 4-62).

---

**4** Provision the VG and Service Mapping profile.

Refer, “[To provision a VG and Service Mapping Profile](#)” (p. 5-137).

---

**5** Configure the following parameters in the NGSS Parameters/Timers screen:

- **Enable VG Session and BW Control**
- **Generate Alarm for VG Session and BW Control**

Refer, “[To provision NGSS Server parameters](#)” (p. 10-9).

END OF STEPS

---

# Provision the Signaling Firewall

## Purpose

This topic provides the provisioning tasks that must be followed to provision the Signaling Firewall.

## Before you begin

The following components must be available and licensed in your system before you can proceed with this procedure:

- P-CSCF
- iSGW-A
- FEPH

## Procedure

Perform the following steps to provision the Signaling Firewall:

- 1 Provision a Trusted default flow policy in the Flow Policy table.  
Refer, “[To provision FEPH Flow Policy](#)” (p. 5-142).
- 2 Review the default policies and policy assignments in the following **FEPH Tables**:
  - 1 Aggregate Flow Policy - The Aggregate Flow Policy is configured to limit the aggregate flow that the FEPH must allow.  
Refer, “[Provision an Aggregate Flow Policy](#)” (p. 5-150).
  - 2 Aggregate Packet Policy - The Aggregate Packet Policy is configured to limit the aggregate packets that the FEPH must allow.  
Refer, “[Provision an Aggregate Packet Policy](#)” (p. 5-147).
  - 3 Aggregate Policy Assignment - The Aggregate Policy Assignment is configured to assign an Aggregate Flow Policy to a specific IMS service and also to assign an Aggregate Packet Policy to a specific IMS service or to the FEPH’s logical pair of internally-facing ethernet ports.  
Refer, “[Provision an Aggregate Policy Assignment](#)” (p. 5-154).
  - 4 Flow Policy - The Flow policy is configured to suit different instances and assigned to the BEPH to be applied for known and unknown flows.  
Refer, “[To provision FEPH Flow Policy](#)” (p. 5-142).
- 3 Provision the Security Gateway.

---

Refer, “[Provision Integrated Security Gateway \(iSGW\)](#)” (p. 1-51).

**Note:**

- From iSGW perspective, the existing SIP rate limits continue to apply regardless of whether TLS is used for TCP transport and the SIP rate limits are applied when TLS is used to carry the SIP messages. The packet level policies applied to the TCP remain the same regardless of whether TLS is used or not and there is no change for the control interface to FEPH.
  - The Keep-Alive mechanism when TLS is used over TCP is the same CRLF keep-alive mechanism for TCP when TLS is not used.
- 

**4 Provision the Security Gateway related parameters in the P-CSCF profile.**

Refer, “[To provision PCSCF profile](#)” (p. 4-77).

END OF STEPS

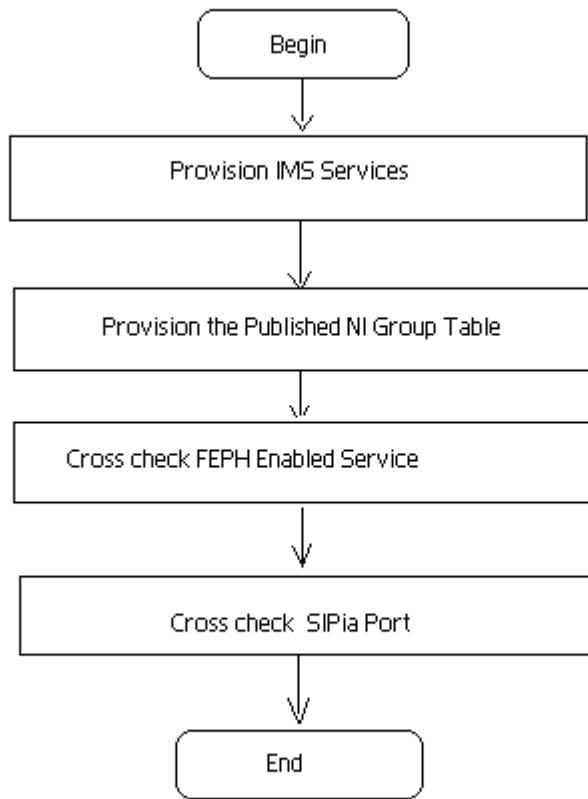
---

# Signaling Firewall Load Balancer or Distribution Function with Single IP Address Exposed for the Gm Interface to End Users - Provisioning Taskflow

## Overview

This topic provides the provisioning taskflow for the feature “Signaling Firewall Load Balancer or Distribution Function with Single IP Address Exposed for the Gm Interface to End Users”.

## Provisioning task flow diagram



## Provisioning procedure

Perform the following steps:

- 
- 1 Provision IMS services.

See “[To provision an IMS Service association](#)” (p. 10-20)

---

- 2 Add the IMS service instance to a Published NI Group. Provision the Published NI Group table.

See “[To provision a Published NI Group Assignment table](#)” (p. 5-230) for more information.

---

- 3 Verify IMS services on the same subnet as FEPH are automatically made FEPH enabled. Cross-check the FEPH Enabled IMS Services.

- 
- 4 Create PCSCF SIPia ports following validation rules. Cross-check the SIPia port.

Cross checks are added for the PCSCF SIPia ports.

If the IMS service associated with the PCSCF is sharing a published NI

- If the P-CSCF has the same Port Number as any of the other PCSCFs in the same Published NI group, then the Port Name must be the same as that of the P-CSCFs..
- Existing rules concerning the SIPia data field values for duplicate Port Names across different IMS services still apply to IMS services that are sharing a Published NI IP with the exception of the ACR Message Generation, Allow Immediate 200 OK, and Area ID fields. Currently, those fields can be set differently for P-CSCFs with the same Port Name on different IMS services. For IMS services that are sharing a Published NI IP, their duplicate P-CSCF Port Names must have the same value for those fields.
- Service-Based PCSCF Profile must be the same for all P-CSCFs in the same Published NI group.
- All PCSCFs in the same Published NI group must have unique TLS Server Port Numbers.
- All PCSCFs in the same Published NI group must not have TLS Server Port Numbers and “SIP” Port Numbers with the same value.
- PCSCF SIPia ports with the same Port Name on IMS services in the same Published NI group can only have the same SIP Permanent Link Set Group Number value if all the SIP Linksets in the group do not have any “Publish” NI values.

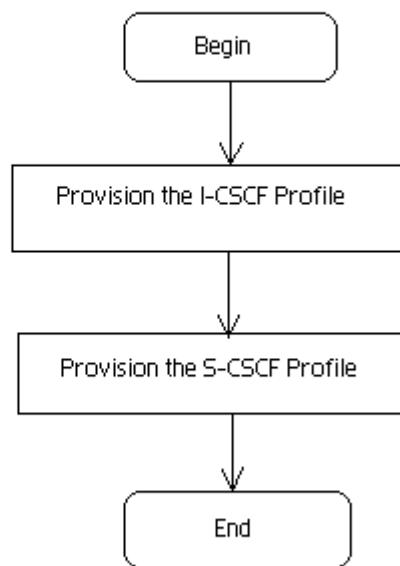
See “[To provision a SIPia port](#)” (p. 10-40)

# Cx Enhancement to support SIP Digest per 3GPP R8 - Provisioning task flow

## Purpose

This topic describes the provisioning task flow that should be followed to support SIP Digest per 3GPP R8.

## Provisioning task flow diagram



## Provisioning steps

Perform the following steps:

- 
- 1 Provision the I-CSCF profile.

On the **I-CSCF Profile Attributes** screen, set the value of the **Register without Authorization Header** parameter to **Derive-PrID**. Refer, “[To provision ICSCF Profile](#)” (p. 4-45).

**Note:** Follow the guidelines below for setting the **Register without Authorization Header** parameter value:

- **Derive PrID** – This is the preferred option when one or more of the following authentication schemes is provisioned:
  - EIS
  - NASS Bundled
  - SIP Digest
- **Set-IMPI-to-Zero** – The ALU HSS will continue to support this option.
  - Should only be used with ALU HSS.
  - Should NOT be used with Digest (PacketCable version) or SIP Digest since in either case the realm needs to be populated using the value from HSS.
- **Reject or Challenge** –
  - Must NOT be used with EIS or NBA.
  - Maybe used with SIP Digest if UE does not send Authorization header and PrID can not be derived from the registering PUID.

---

**2** Provision the S-CSCF profile.

Provision the following parameters on the S-CSCF profile:

- Enable **SIP Digest** as the scheme to be used to authenticate the UE.
- Enable **Support Authentication Info** in the 200 OK to REGISTER request.
- Set the value of **Registration without Authorization header** to **Derive-PrID**.

Refer, “[To provision an S-CSCF profile](#)” (p. 4-15).

# Provisioning Cx Enhancement per 3GPP R7 and R8

## Purpose

This topic describes the procedure to be followed to support the feature “Cx Enhancement per 3GPP R7 and R8”.

## Procedure

Perform the following steps:

---

**1** Provision NGSS Server parameters.

Configure the following parameters on the **NGSS Parameters/Timers Configuration** screen :

- **Support Wildcarded PSI**
- **Include P-Profile-Key**

For more information refer, “[To provision NGSS Server parameters](#)” (p. 10-9).

---

**2** Provision the S-CSCF Profile.

Configure the following parameters on the **S-CSCF Profile Configuration** screen :

- **Support AliasInd**
- **Support Loose-Route-Indication**
- **Guard Timer for Unregistered PUID iFC**
- **Guard Timer for Wildcarded PSI iFC**
- To make WPSI Orig call, configure the parameter **Enable Unregistered Origination**.

For more information refer, “[To provision an S-CSCF profile](#)” (p. 4-15).

---

**3** Provision the I-CSCF Profile.

To make WPSI Tel format call, configure the parameter **Change SIP URI to TEL URI** on the **I-CSCF Profile Attributes** screen.

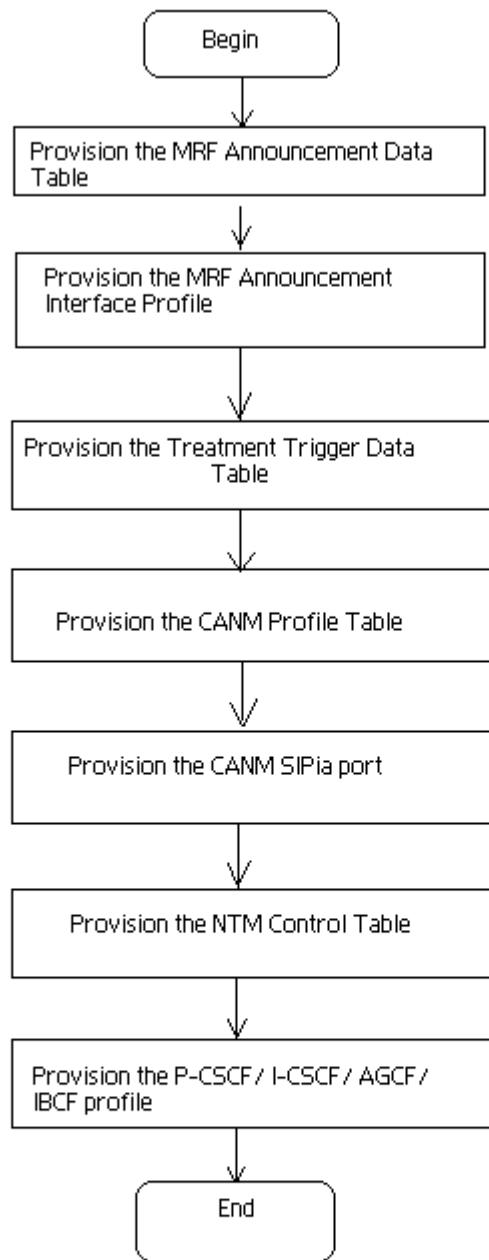
**Note:** Ensure that the option **Use Configured Home Domain in R-URI** is not selected while provisioning this parameter.

For more information refer, “[To provision ICSCF Profile](#)” (p. 4-45).

# Provision Common Announcement Module (CANM) task flow

## Purpose

This topic provides the provisioning task flow that should be followed to provision the support of Common Announcement Module (CANM).

**Provisioning task flow diagram**

## Provision Common Announcement Module (CANM)

Perform the following steps to provision the CANM:

- 1 Provision the MRF Announcement Data table.

Refer, “[To provision MRF Announcement Data table](#)” (p. 4-247).

**Note :** This is an imported table and cannot be added from the GUI.

- 2 Add a new MRF Announcement Interface Profile.

Refer, “[To provision MRF Announcement Interface profile](#)” (p. 4-245).

- 3 Provision the Treatment Trigger Data table.

Refer, “[To provision a Treatment Trigger Data Table](#)” (p. 5-236).

- 4 Provision the CANM Profile table.

Refer, “[To provision a CANM Profile Table](#)” (p. 5-239).

- 5 Provision the CANM SIPia Port.

Select the value **CANM Port** in the **Port Type** drop-down list.

**Note :** The CANM port will be locked by default. The user should enter a valid license to enable CANM SIPia port(s).

By default, the **NTM Control Table** field on the SIPia port configuration will be locked for P-CSCF/ IBCF/ I-CSCF/ AGCF. When the user provisions the **NTM Control Table** field on the SIPia port, a check is made to see if a license for NTM is provisioned and if it is, only then the NTM control table field population is allowed.

Refer, “[To provision a SIPia port](#)” (p. 10-40).

- 6 Provision the NTM Control Table.

Configure the following parameters on NTM Control Table:

- Select the appropriate value from the **Treatment Mechanism** drop-down list.
- Enter the desired value in the **Announcement Treatment ID** field.

**Note:** A non-zero **Announcement Treatment ID** can only be provisioned if the value of the **Treatment Mechanism** field is set to **Announcement**.

Refer, “[To provision an NTM Control table](#)” (p. 4-222).

7 Provision any one of the following profile tables:

- Provision the P-CSCF Profile.

Select the appropriate value from the **CANM URI** drop-down list on the P-CSCF Profile.

Refer, “[To provision PCSCF profile](#)” (p. 4-77).

- Provision the I-CSCF Profile.

Select the appropriate value from the **CANM URI** drop-down list on the I-CSCF Profile.

Refer, “[To provision ICSCF Profile](#)” (p. 4-45).

- Provision the IBCF Profile.

Select the appropriate value from the **CANM URI** drop-down list on the IBCF Profile.

Refer, “[To provision IBCF Profile](#)” (p. 4-198).

- Provision the AGCF Profile.

Select the appropriate value from the **CANM URI** drop-down list on the AGCF Profile.

Refer to the topic, “Provision the iAGCF Profile” in *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420.

**Note:** The **CANM URI** drop-down list will be enabled only if the CANM SIPia port is provisioned.

# BGCF support for Digit Manipulation provisioning task flow

## Purpose

This topic provides the task flow for the support of Digit Manipulation on the BGCF.

## Before you begin

Observe the following:

- Ensure that the IMS Digit table is provisioned before you start this procedure.  
To provision an IMS Digit table refer, "[To provision an IMS Digit Table](#)" (p. 5-110).
- A "DIGANAMANI" feature license is required before proceeding with this procedure.
- This procedure is performed at the FS GUI.

## Provisioning procedure

Perform the following steps:

---

**1 Provision the BGCF Profile table.**

Provision the following parameters on the **Add BGCF Profile Attributes** screen:

- **Digit Table ID**
- **Perform Digit Manipulation in Proxy Mode**
- **Forward request by adding Route Header**

Refer, "[To provision BGCF Profile](#)" (p. 4-142).

---

**2 Provision the BGCF DA Route table.**

Provision the **Digit Table ID** parameter on the **Add DA Route Table Attributes** screen.

Refer, "[To provision BGCF DA Route Table](#)" (p. 4-172).

---

**3 Provision the BGCF Location Based Routing table.**

Provision the **Digit Table ID** parameter on the **BGCF Location Routing Attributes** screen.

Refer, "[To provision BGCF location based routing](#)" (p. 4-189).

---

**4 Provision the BGCF URI table.**

Provision the **Digit Table ID** parameter on the **Target URI Attributes** screen.

---

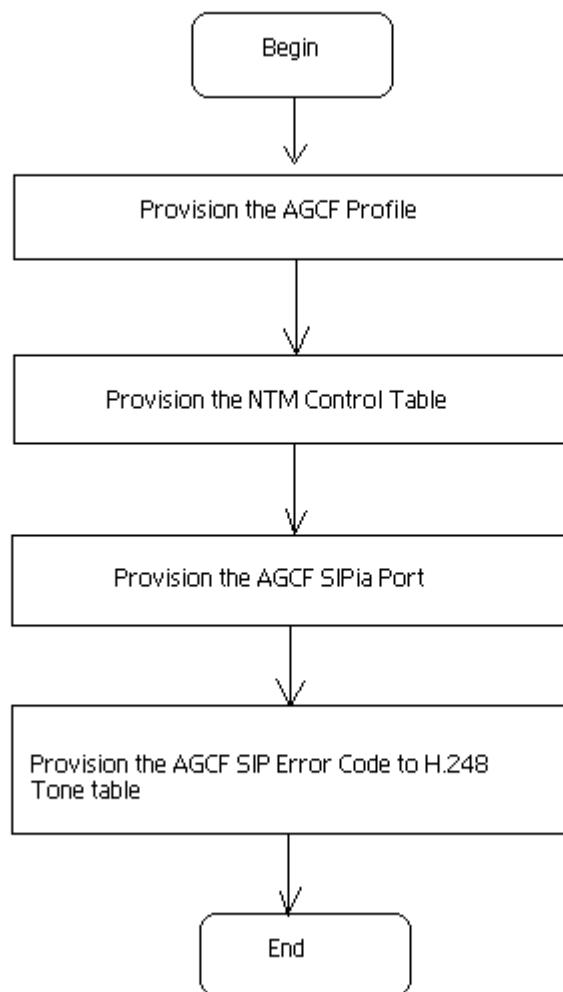
Refer, “To provision BGCF URI Id” (p. 4-133).

# Provision iAGCF support of Network Traffic Management (NTM)

## Purpose

This topic provides the provisioning task flow that should be followed to provision iAGCF support of Network Traffic Management (NTM).

## Provisioning task flow



## Provisioning procedure

Perform the following steps to provision iAGCF support of Network Traffic Management (NTM):

---

**1** Provision the AGCF Profile.

Using the radio buttons in the **Request Rejection Response** field, set the desired request rejection response (Tone or Announcement).

To provision the AGCF profile refer to *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420.

---

**2** Provision the NTM Control Table.

The existing NTM Control Table is modified to produce a warning message if a record that is incompatible with an iAGCF SIPia port (that is currently assigned to the NTM table) is added. The warning message check will only be done when a new field is added since the fields that can be assigned values incompatible to iAGCF cannot be later modified (but must be deleted and added as new fields).

To provision the NTM Control Table refer, “[To provision an NTM Control table](#)” (p. 4-222).

---

**3** Provision the AGCF SIPia port.

It is possible that certain records in the NTM Control Table do not apply to iAGCF SIPia ports and thus will be ignored.

The following types of NTM records do not apply to iAGCF SIPia ports:

- Request Method = REGISTER
- Match Type = User Local Number Format
- Match Type = User Digit Format

When an NTM table is selected for an iAGCF SIPia port and it contains these types of records, a warning message will be produced listing the records that do not apply to iAGCF. The warning will be produced when iAGCF SIPia port has an NTM Control Table ID assigned to it and when the assignment of the Control ID is modified.

To provision the AGCF SIPia Port refer, “[To provision a SIPia port](#)” (p. 10-40).

---

**4** If needed, provision the AGCF SIP Error Code to H.248 Tone table.

---

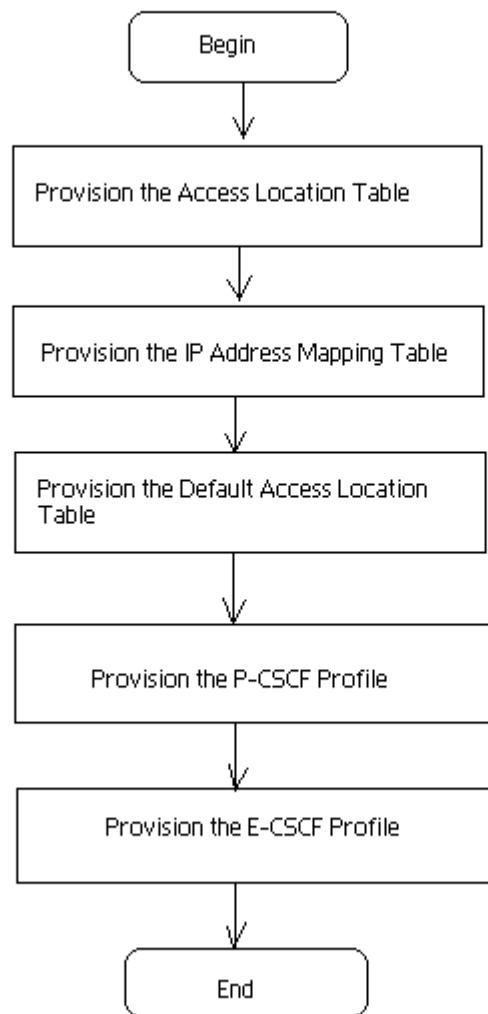
To provision the AGCF SIP Error Code to H.248 Tone table refer, “[To provision an AGCF Cause Code To H248 Tone Table](#)” (p. 5-246).

# CMCC Emergency Service and P-CSCF SIP Header Manipulation provisioning task flow

## Purpose

This topic describes the task flow that should be followed for CMCC Emergency Service and P-CSCF SIP Header Manipulation provisioning.

## Provisioning task flow diagram



## CMCC Emergency Service and P-CSCF SIP Header Manipulation provisioning

- 1 Provision the Access Location to ESRN Mapping table.

Refer, “[To provision an Access Location to ESRN Mapping Table](#)” (p. 5-250).

- 2 Provision the IP Address Mapping table.

Refer, “[To provision an IP Address Mapping Table](#)” (p. 5-255).

- 3 Provision the Default Access Location table.

Refer, “[To provision a Default Access Location Table](#)” (p. 5-259).

- 4 Provision the P-CSCF Profile.

Configure the following parameters on the P-CSCF profile:

- Country Code
- Area Code
- Domain Name for PANI

Refer, “[To provision PCSCF profile](#)” (p. 4-77).

- 5 Provision the E-CSCF Profile.

Provision the **Emergency Service Routing Method** parameter on the E-CSCF Profile.

Select the option **IP-Mapping** from the **Emergency Service Routing Method** drop-down box.

**Note :** When the **Emergency Service Routing Method** parameter is set to **IP-Mapping**, then all the fields in the **VPC Interface** group box will be unavailable. Also, the **T1SPAN/3GPP ECSCF** flag will be checked and the user will not be allowed to change it.

Refer, “[To provision an E-CSCF Profile table](#)” (p. 4-212).

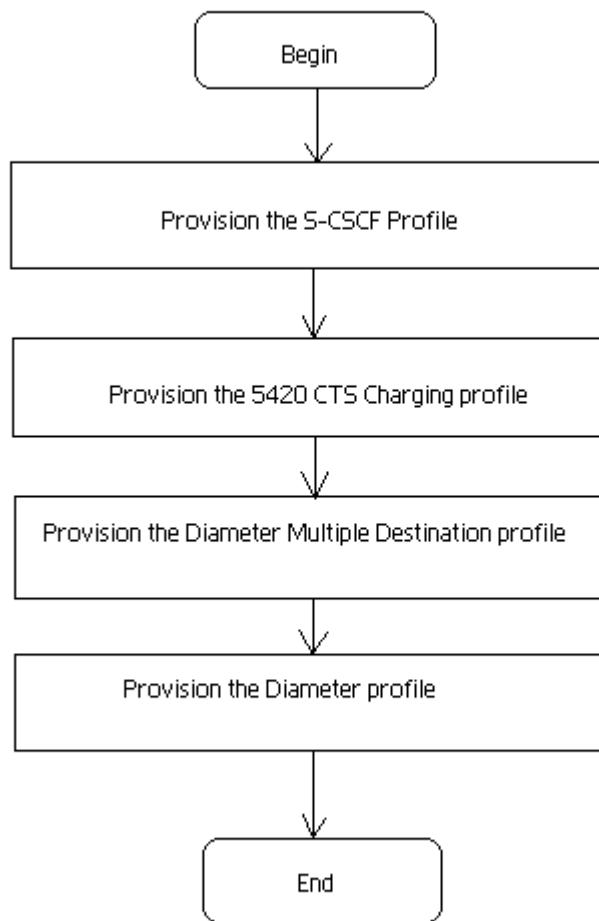
**Note:** The data in the Access Location, IP Mapping and SBC Domain Mapping (Default Access Location) tables will only be sent to NGSS blades defined with a profile that has an ESRM of IP-Mapping.

# Support sending offline charging data to the CCF provisioned to the CTS - Provisioning task flow

## Purpose

This procedure describes the provisioning task flow that must be followed to support sending offline charging data to the CCF provisioned to the CTS.

## Provisioning task flow diagram



## Procedure

Perform the following steps:

---

**1** Provision the S-CSCF profile.

Configure the parameter **Pass HSS Provided CCF address** on the S-CSCF Profile Attributes screen.

For more information, refer “[To provision an S-CSCF profile](#)” (p. 4-15).

---

**2** Provision the 5420 CTS Charging profile.

Configure the parameter **Use HSS Provided CCF Address** on the Charging Profile screen.

Refer to the topic “CTS Charging profile tables”! in *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420.

---

**3** Provision the Diameter Multiple Destination profile.

Configure the parameter **Backup FQDN** on the Diameter Multiple Destination Profile screen.

For more information, refer “[To provision a Diameter Multiple Destination Profile](#)” (p. 4-278).

---

**4** Provision the Diameter profile.

Configure the parameters **Application Type** and **Diameter Multiple Destinations Profile ID** on the Diameter Connection Interface screen.

For more information, refer “[To provision a Diameter profile](#)” (p. 10-23).

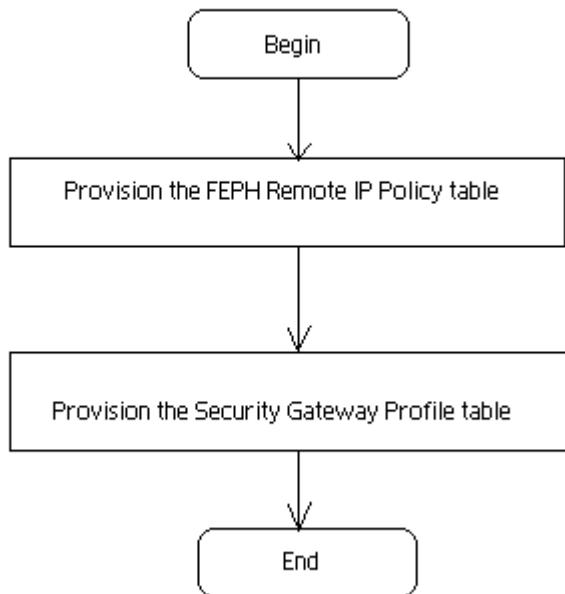
**Note:** The Diameter Multiple Destination profile in the Rf interface supports only CTS service. Do not map it to any other service.

# Limit for TCP Connections - Provisioning

## Purpose

This topic provides the provisioning task flow to be followed to limit the total number of TCP connections (or other connection-oriented connections) per source at transport layer.

## Provisioning task flow diagram



## Provisioning procedure

Perform the following steps:

- 1 Provision the FEPH Remote IP Policy Table.

See “[To provision a Remote IP Policy Table](#)” (p. 5-266) for more information.

- 2 Provision the Security Gateway Profile.

Select the appropriate option from the **Remote IP Policy ID** drop-down list.

See “[To provision a Security Gateway Profile](#)” (p. 5-90) for more information.

# Enhancement of Rx and Gq' interfaces - Provisioning

## Purpose

This topic describes the provisioning procedure to be followed to support the feature “Enhancement of Rx and Gq' interfaces”.

## Procedure

Perform the following steps:

---

**1** Provision the Diameter Profile.

In the diameter profile, it is possible to provision the multiple destination realms for Rx/Gq' interface. In the Diameter Profile table, the **Diameter Multiple Destinations Profile ID** is enabled when the **Application Type** is Rx or Gq'.

See “[To provision a Diameter profile](#)” (p. 10-23) for more information.

---

**2** Provision the SBLP Profile.

Provision the following parameters on the **SBLP Profile Attributes** screen:

- **Reserve Bandwidth per Codec Local Policy**
- **Primary Policy Server Destination FQDN** (TISPAN Parameters)
- **Alternative Policy Server Destination FQDN**(TISPAN Parameters)
- **Primary Policy Server Destination FQDN**(3GPP Parameters)
- **Alternative Policy Server Destination FQDN**(3GPP Parameters)
- **Subscription to Notification of Signaling Path Status**(3GPP Parameters)

See “[To provision the Service Based Local Policy Profile](#)” (p. 4-111) for more information.

---

**3** Provision the P-CSCF Profile.

Enable the **Close Signaling Connection to UE** flag on the **P-CSCF Profile Attributes** screen.

See “[To provision PCSCF profile](#)” (p. 4-77) for more information.

---

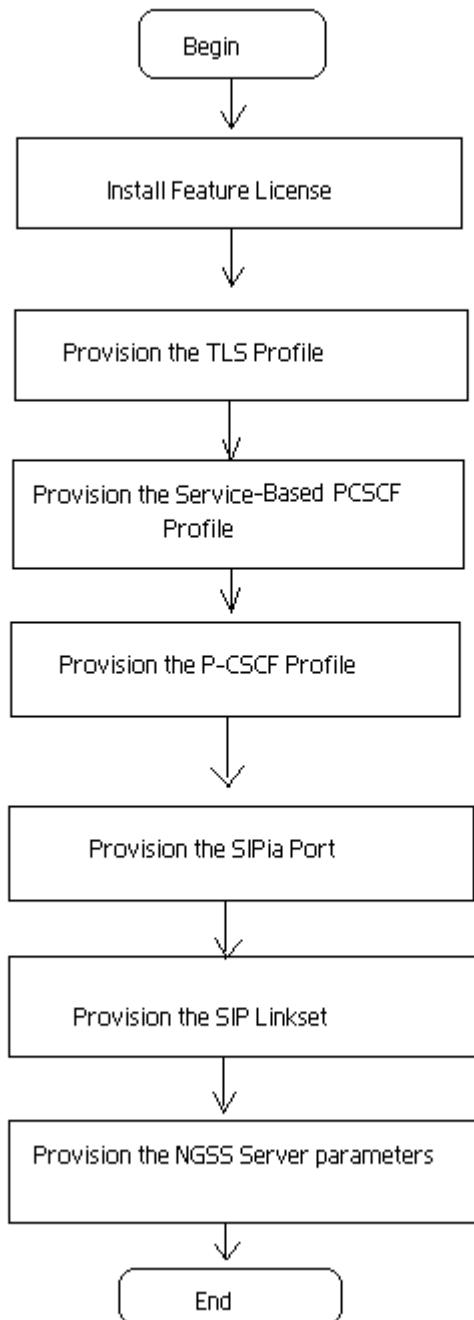
END OF STEPS

---

# Allow SIPS-URI on Gm and Mw Interface - Provisioning

## Purpose

This topic provides the provisioning procedure to be followed to allow SIPS-URI on Gm and Mw Interface.

**Provisioning task flow diagram**

## Provisioning procedure

Perform the following steps:

---

**1** Install the IMS Feature License.

See *Alcatel-Lucent 5450 IP Session Control Software Licenses*, 270-702-029 for more information.

---

**2** Provision the TLS Profile

See “[To provision the TLS Profile table](#)” (p. 4-121) for more information.

---

**3** Provision the Service-Based PCSCF Profile.

Add the TLS profile to Service-Based P-CSCF Profile.

Select the appropriate **TLS Profile ID** from the **Service-Based PCSCF Profile Attributes** screen.

See “[To provision Service-Based PCSCF Profile](#)” (p. 4-69) for more information.

---

**4** Select the desired TLS settings on Gm Interface in the P-CSCF Profile.

Provision the following parameters on the P-CSCF Profile Attributes screen.

- **Convert SIPS URI**
- **TLS Mandatory(Gm Only)**
- **Interface Supports TLS**

See “[To provision PCSCF profile](#)” (p. 4-77) for more information.

---

**5** Provision the SIPia Port.

Provision the following parameters:

- **TLS Server Port Number**
- **Port Profile**
- **Service-Based Profile**

See “[To provision a SIPia port](#)” (p. 10-40)

for more information.

---

**6** Add P-CSCF SIPia Port component to desired IMS service

Provision the SIP Linkset table.

Enable the **TLS** check box.

**Note:** The TLS check box with TCP as transport will configure the Sip Link Set as TLS Link. Only default NI is allowed for TLS link which will configure TLS over Mw. TLS can be used for both destination FQDN or Destination IP address. The Destination FQDN will require DNS query for the FQDN.

See “[To provision an SIP Linkset](#)” (p. 4-264) for more information.

---

7 Provision the NGSS Server parameters.

Under **Global Transport Preference Setting**, configure the values for the following parameters:

- **UDP\_Priority**
- **TCP\_Priority**
- **TLS\_Priority**

See “[To provision NGSS Server parameters](#)” (p. 10-9) for more information.

# IMUX provisioning task flow

## Overview

This provisioning task flow is used to associate the IMUX and IMS components. This involves provisioning of any SIPia port that is used on a shared IP between IMS service and IMUX service on the same host.

IMUX is an optional service that supports shared external IP for SIP communication among the IMS service instances on the same ATCA host. In the absence of IMUX service, the IMS service instances on a host without an IMUX service must each be assigned different external IP addresses.

The IMUX and IMS services on the same host shall share the same external IP addresses.

## Before you begin

Observe the following:

- The IMUX service must be configured in the system.
- IMUX must have the same IP as IMS services on the same host.
- IMS services must be on the same host as IMUX.
- Obtain the feature license for this functionality.

### Important!

1. When IMS services are provisioned with an IMUX on the same host, the same external IP addresses (for example, IPv4 and IPv6) are assigned or shared to the IMUX and each of the IMS services on the host. Note that the internal IP addresses internal IPs are not shared. The IMS SIPia port instances and the IMUX service must each be assigned a different server port for SIP communication. It is recommended that the IMUX is provisioned with at least one SIPia port on IMUX.
2. The IMUX service supports the IPv4 and IPv6 external IP addresses with the following combinations:
  - IPv4 address only
  - IPv6 address only
  - IPv4 and IPv6 addresses

### Note:

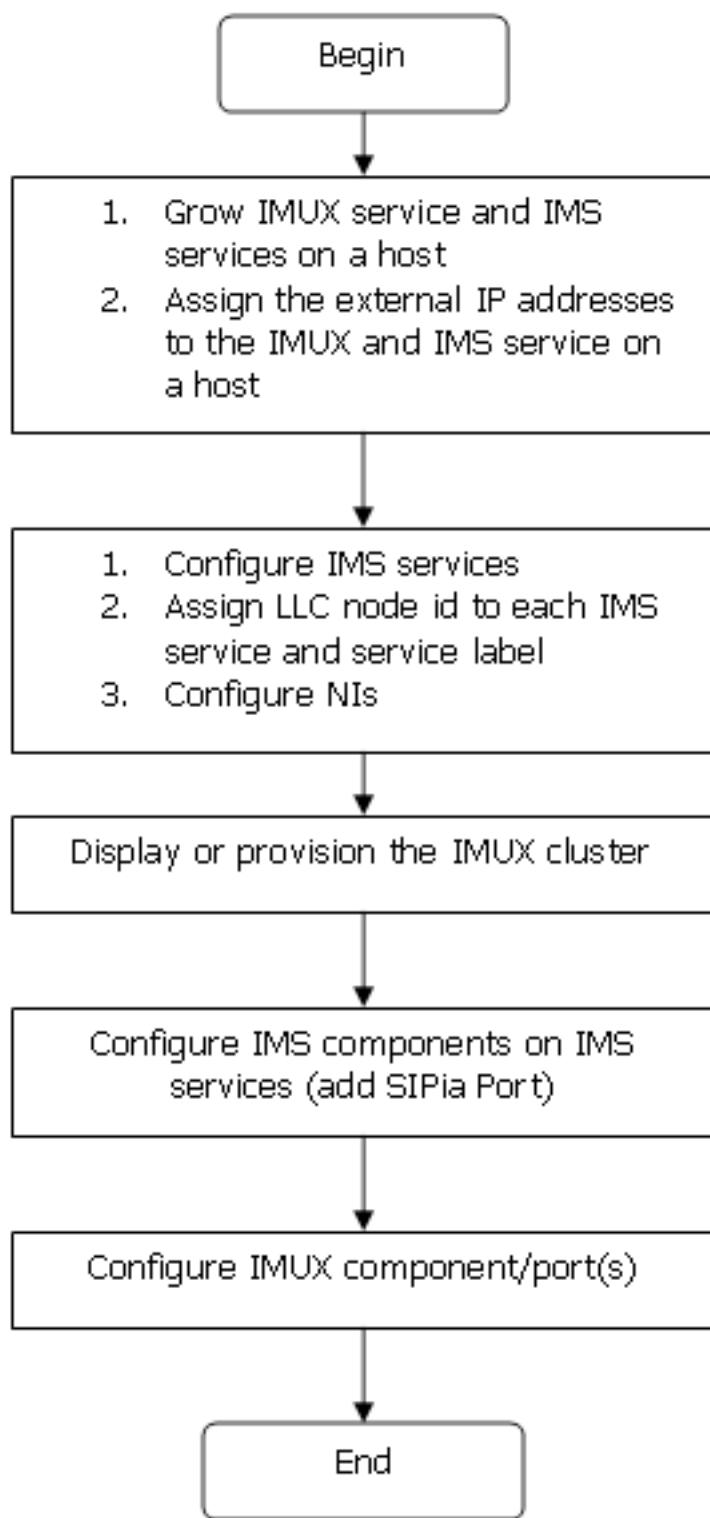
- Addition, or deletion, and modification of default NI is not allowed with exception of adding V4 or V6 when not present.
- Addition, deletion, or modification of IP addresses can be done only when the host is locked.

3. Sharing of external IP addresses is supported for following combinations of NIs, among the IMS services configured on the same host:
  - Default NI, diameter Cx NI, and Rf NI all share the same IP addresses
  - Default NI, diameter Cx NI, and Rf NI all have different IP addresses
  - Diameter Cx and Rf share the same IP addresses that are different from the IP addresses assigned for default NI
4. The IMUX service is supported in an IMS system, on a per host basis.

#### Growth and de-growth of the IMUX service

The IMUX service is configurable as part of the initial system installation procedure. Growth or de-growth of an IMUX or IMS in a live system is not supported. The IMUX supports the growth and de-growth of an IMS service within a cluster. The support is provided only when the cluster is not in service. The IMS component needs to be configured on an IMS service within the cluster first, before it can be added to the IMUX server port.

## Provisioning task flow



## To provision the IMUX component

The tasks for provisioning IMUX and IMS components to a cluster on a host are as follows:

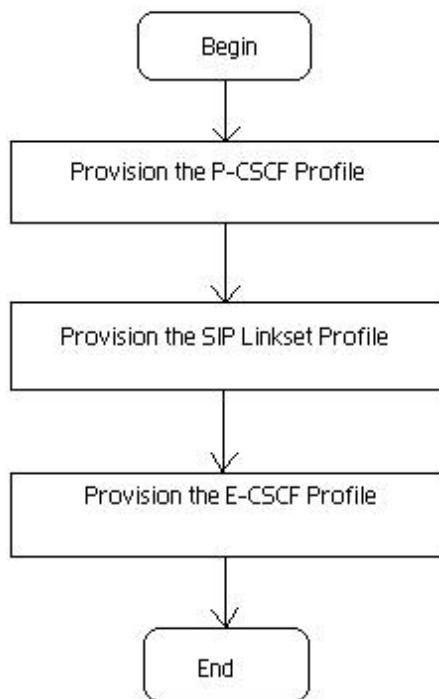
- 1 Grow IMUX service and IMS services on a host (use SCDT and MI GUI).  
Assign the same external IP addresses to the IMUX and IMS service on a host.
- 2 Provision IMS services, assign LLC node id to each IMS service and service label.  
See the topic, "*The System View window introduction*" in the *ISC Application User Guide*.
- 3 Provision an IMS service whose default NI external floating v4/v6 IP address combination is the same as the IMUX's default NI external floating v4/v6 IP address combination.  
Automatically, the cluster that consists of IMS services and the IMUX service on the same host sharing the same external IP addresses is displayed. This list is used to verify if the association is successful.  
Add and delete actions must be supported to add or delete IMS services to an IMUX cluster.  
See: "[To provision IMUX to IMS Association Table](#)" (p. 5-271)
- 4 Provision IMS components on IMS services by adding SIPia Ports. Cross-check to ensure that the server port number (port number in SIPia Port) is assigned to IMS components on each IMS service is different within a cluster. The server port number can be shared by IMS components on an IMS service, for example, I-CSCF and S-CSCF on an IMS service can share the same port number.  
See: "[To provision a SIPia port](#)" (p. 10-40)  
**Note:** For IMS services that are not in a cluster, the IMS components using the same SIPia profile share the same server port number.
- 5 Provision the IMUX port(s).  
See: "[To provision IMUX port](#)" (p. 5-274)

# Provisioning Support of the NENA V5 SIP Interface to LRF and EATF for SRVCC

## Purpose

This topic provides the provisioning task flow that should be followed to provision Emergency Enhancement for AT&T and UVP Applications.

## Provisioning task flow diagram



## Provisioning procedure

Perform the following steps:

- 1 Provision the P-CSCF Profile.

On the **Miscellaneous Parameters** tab of the P-CSCF Profile, provision the parameter **XML Body in 380**.

See “[To provision PCSCF profile](#)” (p. 4-77) for more information.

---

**2** Provision the SIP Link Set Profile.

On the **General Parameters** tab of the SIP Link Set Profile, provision the following parameters:

- **User part of R-URI and TO header in OPTIONS**
- **User part of FROM header in OPTIONS**

See “[To provision an SIP Linkset](#)” (p. 4-264) for more information.

---

**3** Provision the E-CSCF Profile.

On the **Routing Methods** tab of the E-CSCF Profile, provision the following parameters:

- In the **Emergency Session Routing Method**, select **V5-LRF** as the ESRM value.
- **V5 LRF FQDN**
- **EATF FQDN**

See “[To provision an E-CSCF Profile table](#)” (p. 4-212) for more information.

# Provisioning - Support MSRP Peak Data Rate to Enhance User Experience

## Purpose

This provisioning task flow provides the steps for provisioning MSRP Peak Data Rate to enhance user experience.

## Procedure

Perform the following steps:

---

### 1 Provision the SBLP Profile

Provision the following parameters:

- **Peak Bandwidth** - Specify the Peak Bandwidth for audio(uplink and downlink), video(uplink and downlink), message(uplink and downlink) and other(uplink and downlink).
- **Max Burst Size** - Specify the Max Burst Size for audio(uplink and downlink), video(uplink and downlink), message(uplink and downlink) and other(uplink and downlink).
- **Reserve Bandwidth per SDP Local Policy**
- **Enhanced Data Rate Control per Local Policy**

See “[To provision the Service Based Local Policy Profile](#)” (p. 4-111) for more information.

---

### 2 Provision the SDP Profile

Provision the following parameters under **Bandwidth Allowed Per Codec**:

- **Default Audio Codec Peak Bandwidth**
- **Default Audio Codec Max Burst Size**
- **Default Video Codec Peak Bandwidth**
- **Default Video Codec Max Burst Size**

Provision the following parameters under **Bandwidth Allowed Per MSRP Media Type**:

- **Default MSRP Media Type Bandwidth**
- **Default MSRP Media Type Peak Bandwidth**
- **Default MSRP Media Type Max Burst Size**

See “[To provision a Session Description Protocol Profile](#)” (p. 4-62) for more information.

---

**3** Provision the SDP Media MSRP table

Provision the following parameters:

- **ID**
- **Media Type**

See “[To provision an SDP Media MSRP Table](#)” (p. 5-286) for more information.

---

**4** Provision the SDP Media Component Policy Profile

- **Attribute MSRP Media Type Policy Treatment** - It specifies whether the treatment for the listed MSRP media type is allowed or disallowed. Allowed means only media types listed are allowed and Disallowed means only media types listed are blocked.
- **SDP Media Component Policy MSRP Media Type** - It specifies the content of the MSRP media type, like text, image, audio, video, application, multipart, message and so on.

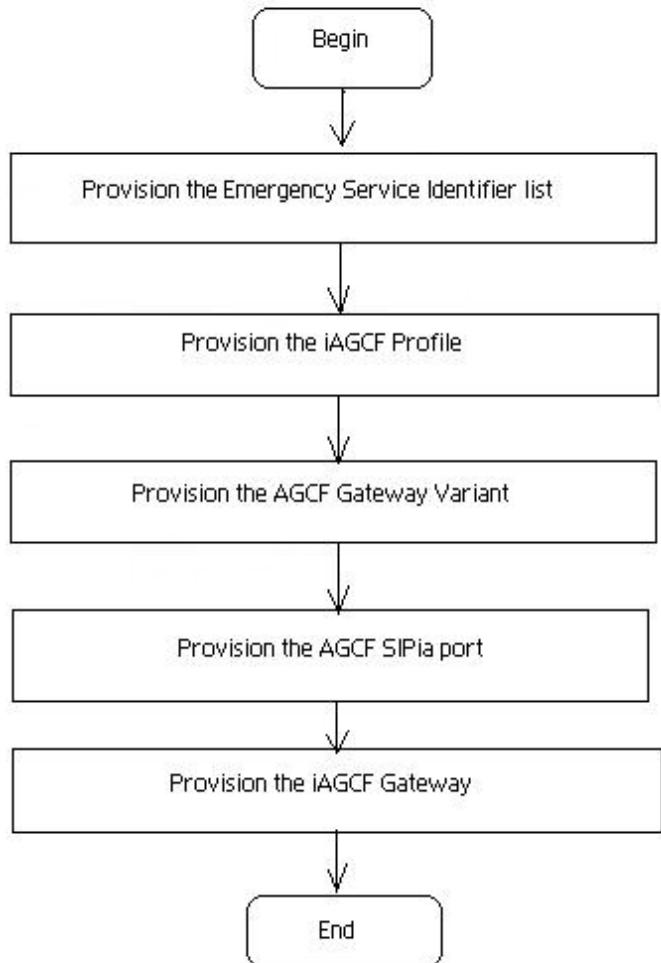
See “[To provision SDP media](#)” (p. 4-6) for more information.

# Provisioning - iAGCF Support of a Large Number of Residential Gateways

## Purpose

This provisioning task flow describes the procedure to provision iAGCF support of a large number of residential gateways.

## Provisioning task flow diagram



## Procedure

Perform the following steps:

- 
- 1 Provision the Emergency Service Identifier list.

See “[To provision an Emergency Identifiers List](#)” (p. 5-61) for more information.

---

- 2 Provision the iAGCF Profile.

Provision the following parameters:

- Enable the **Gateway Registration Rate Limit** check box to control whether the iAGCF should limit the gateway H.248 registration message rate.
- **Number of H.248 Registration Allowed per Interval** - The iAGCF supports provisioning of this field if the **Gateway Registration Rate Limit** is set to “Yes”.
- **H.248 Registration Monitoring Interval** - This field defines the time interval that the iAGCF takes to monitor the H.248 registration rate for analog lines.
- **Suppress Group Alarms** - This option controls whether the iAGCF suppresses the following alarms:
  - LSS\_gatewayUnregistered
  - LSS\_gatewayForcedOOS
  - LSS\_gatewayUnreachable
  - LSS\_gatewayCongestion for a RGW/iAD gateway group on one iAGCF service.

**Note:** The GWs in one RGW/iAD group may be distributed on multiple iAGCF services, so there is a possibility that the alarm is suppressed for GWs in one group on one iAGCF, but the alarm can still be fired for GWs in the same group on another iAGCF. This is not a recommended configuration.

See *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420 for more information.

---

- 3 Provision the AGCF Gateway Variant.

Provision the following parameters:

- **Variant ID** - To support large number of RGWs/iADs, the number of gateway variants is increased to 256.
- **Vender ID** - This field specifies the vender identity which is used for applying special vender handling on the iAGCF per gateway, Zero (0) value means no special vender handling is applied. A non-zero value identifies the vender specific handling that is done.

- **Heartbeat Timer** - This field specifies the interval of the heartbeat between the iAGCF and the gateways. Heartbeat failure can trigger gateway de-registration
- **Identify Gateway by mID** - This field controls whether the iAGCF uses H.248 message ID to identify a GW. Per H.248 specific message ID can have Device Name, Domain Name, Domain Address and so on. When this field is set to “Yes”, either Domain Name or Domain Address can be used. Domain Address is only used if an IP address is provisioned for an AGW/RGW. If this field is set to “No” (typical for AGWs), then the AGCF continues to use the source IP of the UDP (like today) to identify AGW and accept packets from the provisioned IP of the AGW/RGW.
- **Gateway mID Domain** - This field defines the domain portion used in H.248 message ID for gateway.
- **AGCF mID Type** - This field defines how to populate H.248 message ID while the iAGCF sends requests/replies/ACKs.
- **Concatenation Separator** - This field defines the character string used to concatenate the GW message ID with iAGCF domain name. When set to NULL, it means GW message ID are not concatenated. Characters allowed in this must be within the range of characters defined for the mID syntax except character “.” is not allowed.

See *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420 for more information.

---

**4** Provision the AGCF SIPia port.

See “[To provision a SIPia port](#)” (p. 10-40) for more information.

---

**5** Provision the iAGCF Gateway.

Provision the following parameters

- **UDP/IP Port** - This field specifies the UDP/IP port used by a gateway.
- **Gateway Type** - This field specifies if the gateway is an Access Gateway (AGW) or a Residential Gateway (RGW) / Integrated Access Device (iAD). Once a GW has been provisioned, the **Gateway Type** field cannot be changed.
- **Gateway ID** - This field defines the identity per GW.
- **Gateway Group ID** - This field defines the ID of the group which this gateway belongs to.
- **SIP Domain Name** - This field replaced the existing field **Gateway Domain** to specify the domain associated with the gateway.
- **Send Compact Messages** - This field defines whether to send compact form text encoding H.248 signaling.

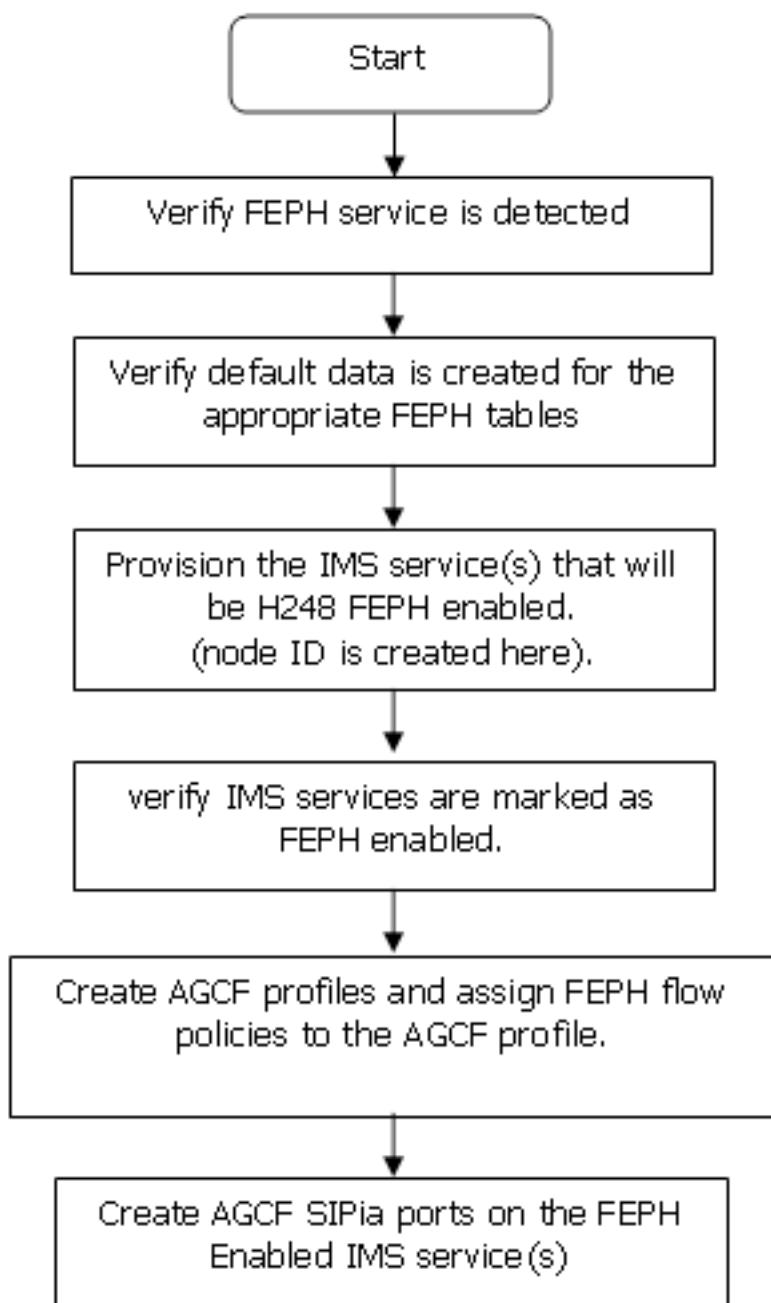
---

See *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420 for more information.

# Provisioning the border access capability for H.248 interface

## Purpose

This provisioning task flow describes the procedure to provision for the border access capability for H.248 interface

**Provisioning task flow diagram****Description**

In the Provisioning GUI, the SIPia port, Flow Policy, and P-CSCF profile have the following impacts:

**SIPia port:** The Security IP Filtering Mask for Inbound Traffic fields are enabled for AGCF SIPia ports and the Enable Two NIIs field continues to be disabled for AGCF SIPia ports. See “[To provision a SIPia port](#)” (p. 10-40)

**Flow Policy:** Apart from the three default flow policy records that are created for SIP (ids 1-3), three new default records are created for H248 usage. Records in this table are assigned to the Security Gateway Profile (FEPH Policies) and the AGCF Profile. See “[To provision FEPH Flow Policy](#)” (p. 5-142)

**P-CSCF Profile:** The “Insert Priority Header for Emergency Calls” field is added and the Access Type field has additional range. See “[To provision PCSCF profile](#)” (p. 4-77)

### BGCF Tables:

The BGCF PANI Access Type field has additional range. The default access type items is 38. The available character set for access type is: ASCII 0x20-0x7e except for “” and “/”.

The BGCF PANI Access Info field has additional range. The default access type items is 10. The available character set for access type is: ASCII 0x20-0x7e except for “” and “/”. BGCF Location routing refers to BGCF PANI access type and PANI access info. See “[To provision BGCF location based routing](#)” (p. 4-189).

**NGSS Parameters:** The “Domain Type for PANI” field is added into NGSS Parameters. See “[To provision NGSS Server parameters](#)” (p. 10-9)

New provisioning fields are provided in the iAGCF Profile, AGCF Gateway, AGCF Gateway Variant screens

The iAGCF Profile is added with the following new fields:

- Insert Priority header for Emergency calls
- Default Inbound FEPH Policy Index
- Default Inbound FEPH Policy Timeout
- Default Outbound FEPH Policy Index
- Default Outbound FEPH Policy Timeout
- FEPH Remote IP Policy Index
- Gateway Registration Rate Limit
- Number of H.248 Registration Allowed per Interval
- H.248 Registration Monitoring Interval
- Number of Allowed Concurrent Sessions
- Suppress Group Alarms

The AGCF Gateway Variant has the following new fields:

- Variant Id
- Digit Map Handling
- Request Digit Collection After Offhook

- Add PANI Header
- Access Type
- Domain Name for PANI
- Query Supported Packages on GW
- Analog Line Alerting Signal
- Network Failure Detection
- Lazy Arming/Initialization Restart Cold Boot
- Lazy Arming/Initialization Disconnect Service Change
- Lazy Arming/Initialization Handoff Service Change
- Arming/Initialization Failover Service Change
- Lazy Arming/Initialization Send Arming in Wildcard Modify
- Channel Status Audit Timer

For more information, see *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420

# Access border for IMS or Pre-IMS core provisioning task flow

## Purpose

This topic describes the task flow that should be followed for provisioning the Access border for IMS or Pre-IMS core

## Before you begin

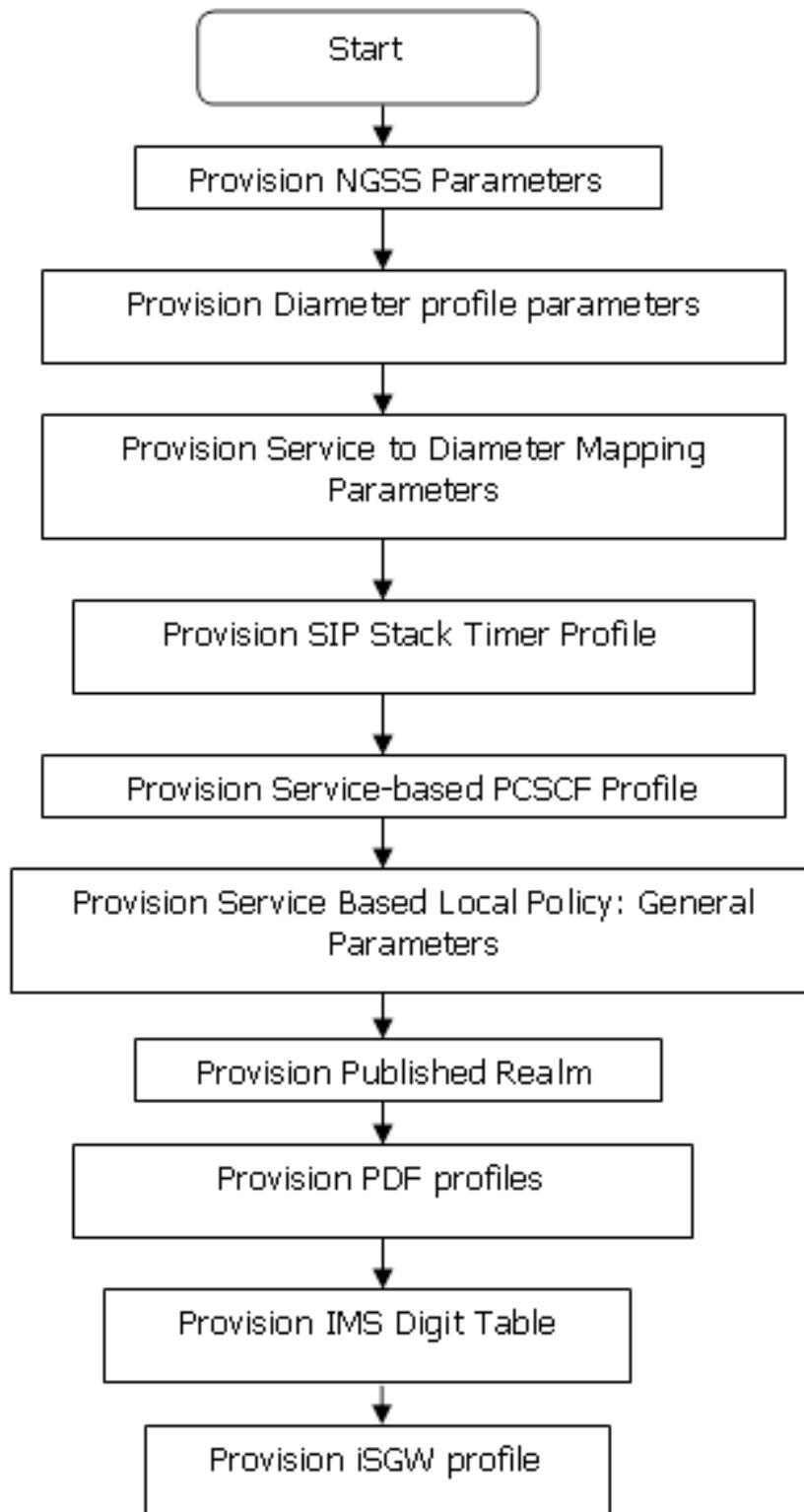
Ensure the following:

- For 5450 ISC, the system has been installed with published NI for IMS services running “non-3GPP IBC” or “3GPP IBC”
- For 5060 IBC4, “full IBC-4” installation (include running “xmlprovims” and OMC-P wizard) has been done

The following software feature license should have been installed

- Virtual GroupVirtual Group (VG)
- P-CSCF (PCSCF)
- IPv6 (IIPv6)
- FEPH (FEPH)
- iSGW (iSGW-A)
- NTM (NTM)
- Rf (IRf)
- SIP Screening (IScreen-A)
- iCCF (ICCFperSub)
- Digit Manipulation (DIGANAMANI)
- SPDF (pdfe)

### Basic configuration task flow diagram



## Basic configuration task flow

This part covers the GUI provisioning to support the new “non-3GPP IBC” or “3GPP IBC”.

---

### 1 Provision the NGSS parameters > Screen 1 parameters

Provision the following parameters:

- Default Home Domain
- Authentication Realm
- Home I-CSCF

**Note:** Provisioning the “Home I-CSCF” is just to satisfy GUI cross-check

Enable the following:

- Enable VG Session and BW Control
- Generate Alarm for VG Session and BW Control

See “[To provision NGSS Server parameters](#)” (p. 10-9)

---

### 2 Provision the NGSS parameters > Screen 2 parameters.

Enable the following:

- SIP Session Parameter
- Send 100 Trying in response to non-INVITE request
- Immediately send 100 Trying in response to MESSAGE
- SIP Message Screening

Enter the **Topology Hiding Host String** field with any “host” for topology hiding purpose.

See “[To provision NGSS Server parameters](#)” (p. 10-9)

---

### 3 Provision the Diameter profile parameters

Add a diameter profile with “Rf” interface

See “[To provision a Diameter profile](#)” (p. 10-23)

---

### 4 Provision the Service to Diameter Mapping

Set mapping between diameter profile and IMS service

See “[To provision a Service to Diameter mapping](#)” (p. 10-32)

---

**5** Provision the SIP Stack Timer Profile as follows:

SIP Stack Timer profile 1 (for access side): Use the default T1 2000 ms, and T2 16 sec.  
FTGT not needed for access side

See “[To provision SIP Stack Timer Profile](#)” (p. 4-74)

---

**6** Provision the Service-based PCSCF Profile

See “[To provision Service-Based PCSCF Profile](#)” (p. 4-69)

---

**7** Provision the Service Based Local Policy > General Parameters:

Change “Diameter Interface Type” to “TISPAN”

See “[To provision the Service Based Local Policy Profile](#)” (p. 4-111)

---

**8** Provision the Service Based Local Policy: TISPAN Parameters

1. Set “Policy Server FQDN” to PDFE’s host name
2. Turn on “Detect Far End NAT”

See “[To provision the Service Based Local Policy Profile](#)” (p. 4-111)

---

**9** Provision the Published Realm

Add one publish realm. This will be used in P-CSCF profile.

See “[To provision a Published Realm](#)” (p. 4-286)

---

**10** Provision the PDF profiles

Add one PDFE profile with “Diameter Interface Type” as “TISPAN”.

See “[To provision a PDF profile](#)” (p. 10-104)

---

**11** Provision the IMS Digit Table only for non-3GPP IBC.

Add IMS digit table for “digit manipulation” purpose. This will be used in “IBC route profile”.

See “[To provision an IMS Digit Table](#)” (p. 5-110)

---

**12** Provision the Service Based Local Policy > General Parameters:

---

Change “Diameter Interface Type” to “TISPAN”

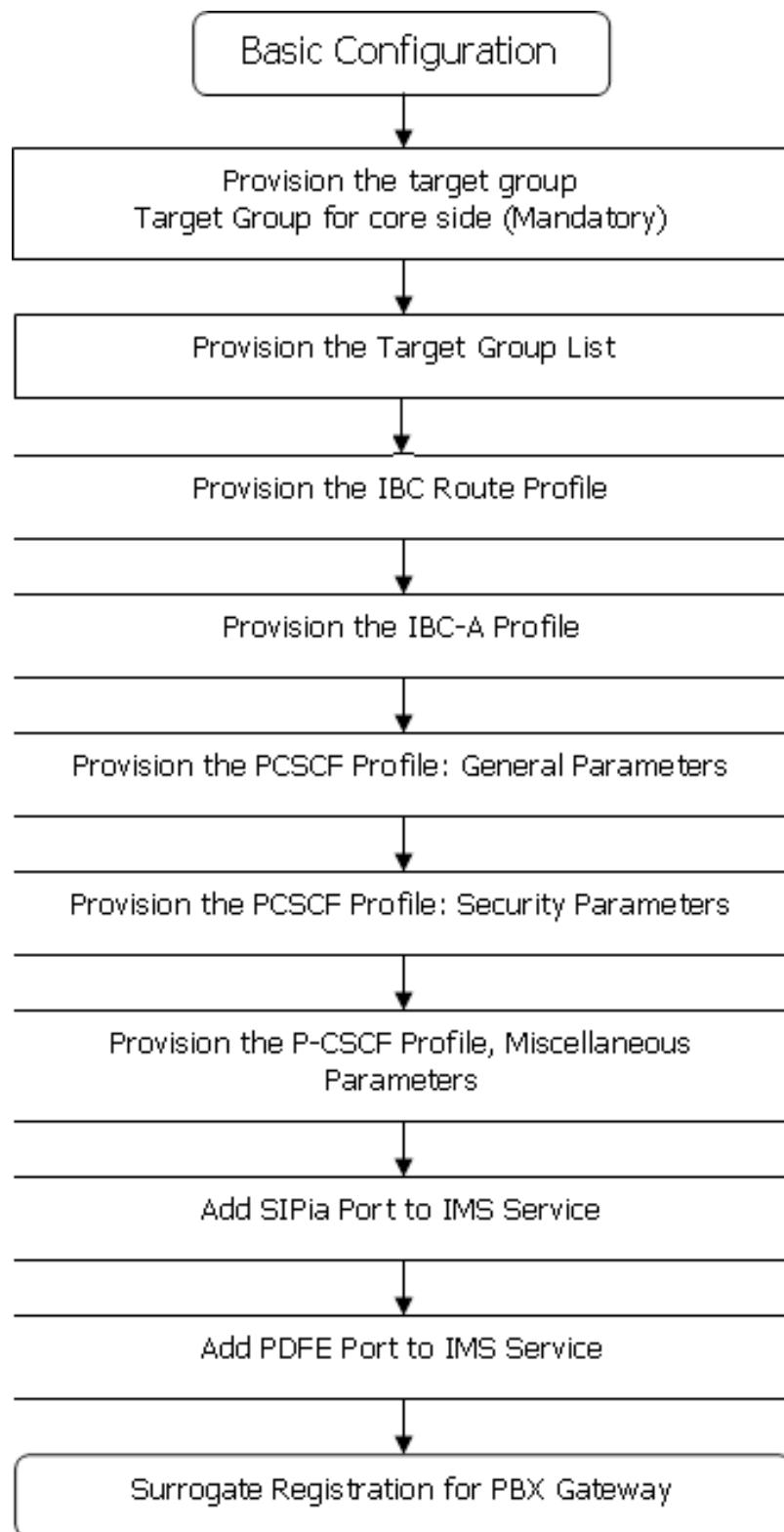
See “To provision the Service Based Local Policy Profile” (p. 4-111)

---

- 13** Provision an iSGW profile.

See “Provision Integrated Security Gateway (iSGW)” (p. 1-51)

## 3GPP IBC Configuration task flow diagram



## 3GPP IBC Configuration task flow

This part includes all new GUI provisioning introduced by this feature. Both 5450 ISC and 5060 IBC-4 need reference this part to support “3GPP IBC”.

### 1 Provision the Target Group for core side.

This step is mandatory and to define the next hop information to core from “3GPP IBC” introduced in this feature.

Provision the Target group parameters for core side as follows:

- Location: “Core”
- Target Type: IPv4/IPv6/FQDN
- Enable Heartbeat: enabled

See “[To provision Target Group Table](#)” (p. 5-304)

### 2 Provision the Target Group List

After defining target group, target group list can be created with existing target groups.

See “[To provision Target Group Table](#)” (p. 5-304)

### 3 Provision the following IBC Route Profile parameters:

- Default proxy
- Domain Match

See “[To provision IBC Route Profile](#)” (p. 5-297)

### 4 Provision the following IBC-A Profile parameters:

- Apply Privacy: (recommended value is Yes)
- Provide P-CSCF IP Address to Core: (recommended value is Yes)
- Support 3xx: (recommended value is No)
- Disable 3GPP Headers: (recommended value is No)
- Contact Rewrite: (recommended value is Yes)
- Path header not included: (recommended value is Yes)
- Don’t Subscribe to ‘reg’ Event: (recommended value is Yes)
- Service-Route not required: (recommended value is No)
- P-Associated-URI not required: (recommended value is No)
- Use Derived Private-ID: (recommended value is No)

- Use Registry Cache Data: (recommended value is Yes)
- Allow Unregistered Calls: (recommended value is Emergency Only)
- Insert ue-addr: IBC-0360 (recommended value is Yes)

See “[To provision IBC-A Profile](#)” (p. 5-290)

---

**5 Provision the PCSCF Profile: General Parameters**

- Provide P-CSCF IP Address to UE
- Encode Contact Data
- Activate SIP Header Reduction
- UDP Symmetric Response Routing
- End-to-End Treatment for BYE
- SIP Topology Hiding
- IBC-Access Mode: “3GPP IBC”
- IBC-A Profile ID: set as above created in IBC-A Profile
- Published Realm: set as above created “published realm”
- Registration Suppression only when NAT detected
- Apply Registration Suppression only when NAT detected

See “[To provision PCSCF profile](#)” (p. 4-77)

---

**6 Provision the PCSCF Profile: Security Parameters.**

IP Association (granularity: IP Address and Port) must be enabled for Non-3GPP IBC.

See “[To provision PCSCF profile](#)” (p. 4-77)

---

**7 Provision the P-CSCF Profile, Miscellaneous Parameters**

- Turn on “SBLP Enabled”
- Associate the SBLP profile with SBLP profile ID

See “[To provision PCSCF profile](#)” (p. 4-77)

---

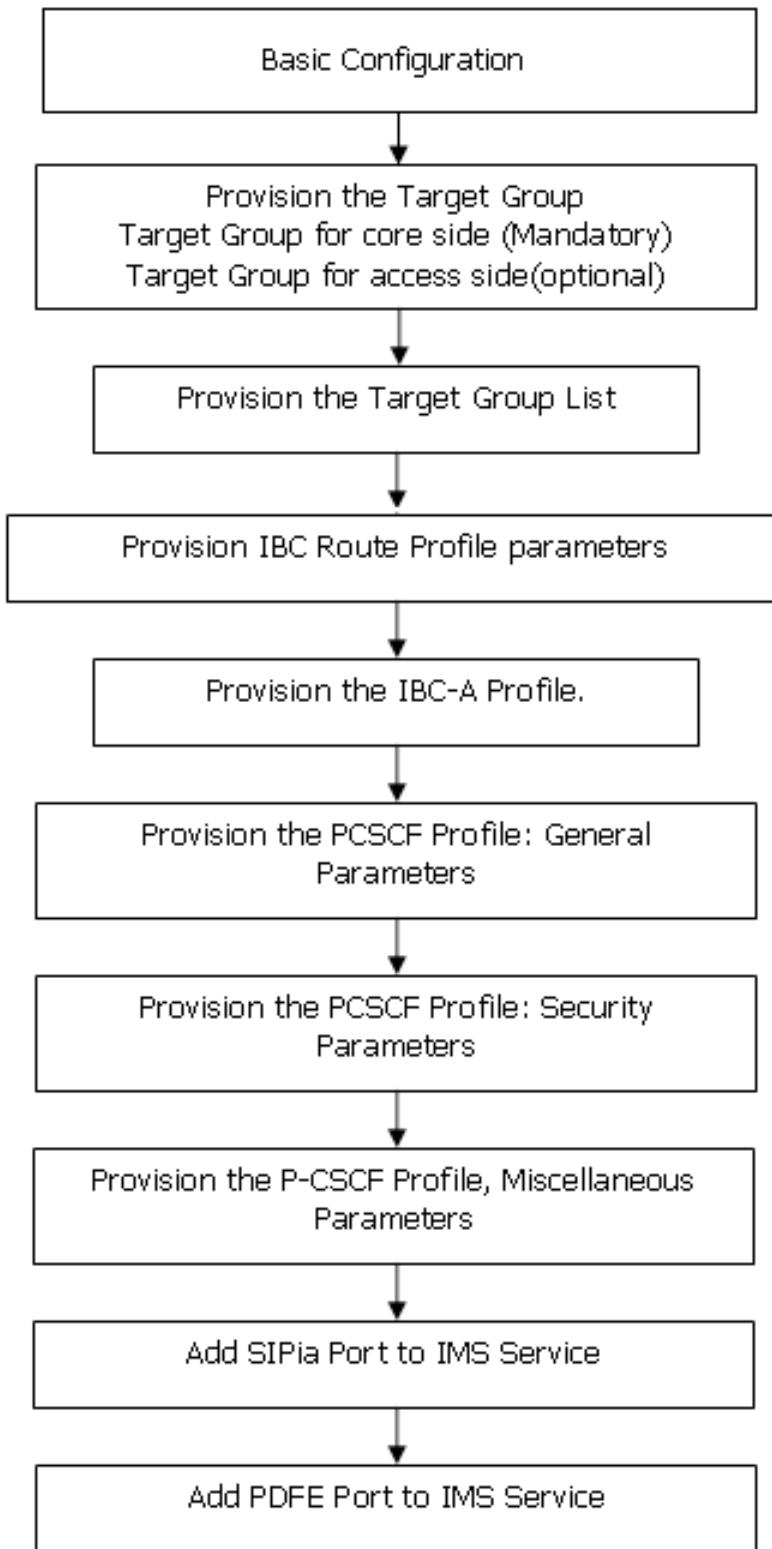
**8 Add SIPia Port to IMS Service**

- Select the above defined “P-CSCF Profile” and “Service-based P-CSCF Profile”
- Enable Two NIs for SIP
- Enable “ACR Messages Generation”

See “[To provision a SIPia port](#)” (p. 10-40)

- 
- 9 Add PDFE Port to IMS Service.

See “To provision a Diameter port” (p. 10-108)

**Non-3GPP IBC Configuration task flow diagram**

## Non-3GPP IBC Configuration task flow

This part includes all new GUI provisioning introduced by this feature. Both 5450 ISC and 5060 IBC-4 need reference this part to support “non-3GPP IBC”.

---

### 1 Provision the Target Group for core side.

This step is mandatory and to define the next hop information to core from “non-3GPP IBC” introduced in this feature.

Provision the Target group parameters for core side as follows:

- Location: “Core”
- Target Type: IPv4/IPv6/FQDN
- Enable Heartbeat: enabled

See “[To provision Target Group Table](#)” (p. 5-304)

---

### 2 Provision Target Group for access side

This step is optional and to define next hop to access side from “non-3GPP IBC” introduced by this feature. It is for unregistered termination purpose.

“Service Label” and “P-CSCF GUL” must be filled with existing “service label” and PCSCF SIPia Port name.

See “[To provision Target Group Table](#)” (p. 5-304)

---

### 3 Provision the Target Group List

After defining target group, target group list can be created with existing target groups.

See “[To provision Target Group List](#)” (p. 5-310)

---

### 4 Provision the following IBC Route Profile parameters:

- digit manipulation
- domain rewrite
- trunk group rewrite
- domain based routing
- trunk group based routing
- default proxy

See “[To provision IBC Route Profile](#)” (p. 5-297)

---

**5 Provision the IBC-A Profile.**

See “[To provision IBC-A Profile](#)” (p. 5-290)

---

**6 Provision the PCSCF Profile: General Parameters**

- Provide P-CSCF IP Address to UE
- Encode Contact Data
- Activate SIP Header Reduction
- UDP Symmetric Response Routing
- End-to-End Treatment for BYE
- SIP Topology Hiding
- IBC-Access Mode: “Non-3GPP IBC”
- IBC-A Profile ID: set as above created in IBC-A Profile
- Published Realm: set as above created “published realm”
- “Registration Suppression only when NAT detected”
- “Apply Registration Suppression only when NAT detected”

See “[To provision PCSCF profile](#)” (p. 4-77)

---

**7 Provision the PCSCF Profile: Security Parameters**

Provision the Security Gateway Profile Id parameter.

IP Association (granularity: IP Address and Port) should be enabled for Non-3GPP IBC.

See “[To provision PCSCF profile](#)” (p. 4-77)

---

**8 Provision the P-CSCF Profile, Miscellaneous Parameters**

- Turn on “SBLP Enabled”
- Associated the SBLP profile with SBLP profile ID

See “[To provision PCSCF profile](#)” (p. 4-77)

---

**9 Add SIPia Port to IMS Service**

- Select the above defined “P-CSCF Profile” and “Service-based P-CSCF Profile”
- Enable Two NIIs for SIP
- Enable “ACR Messages Generation”

See “[To provision a SIPia port](#)” (p. 10-40)

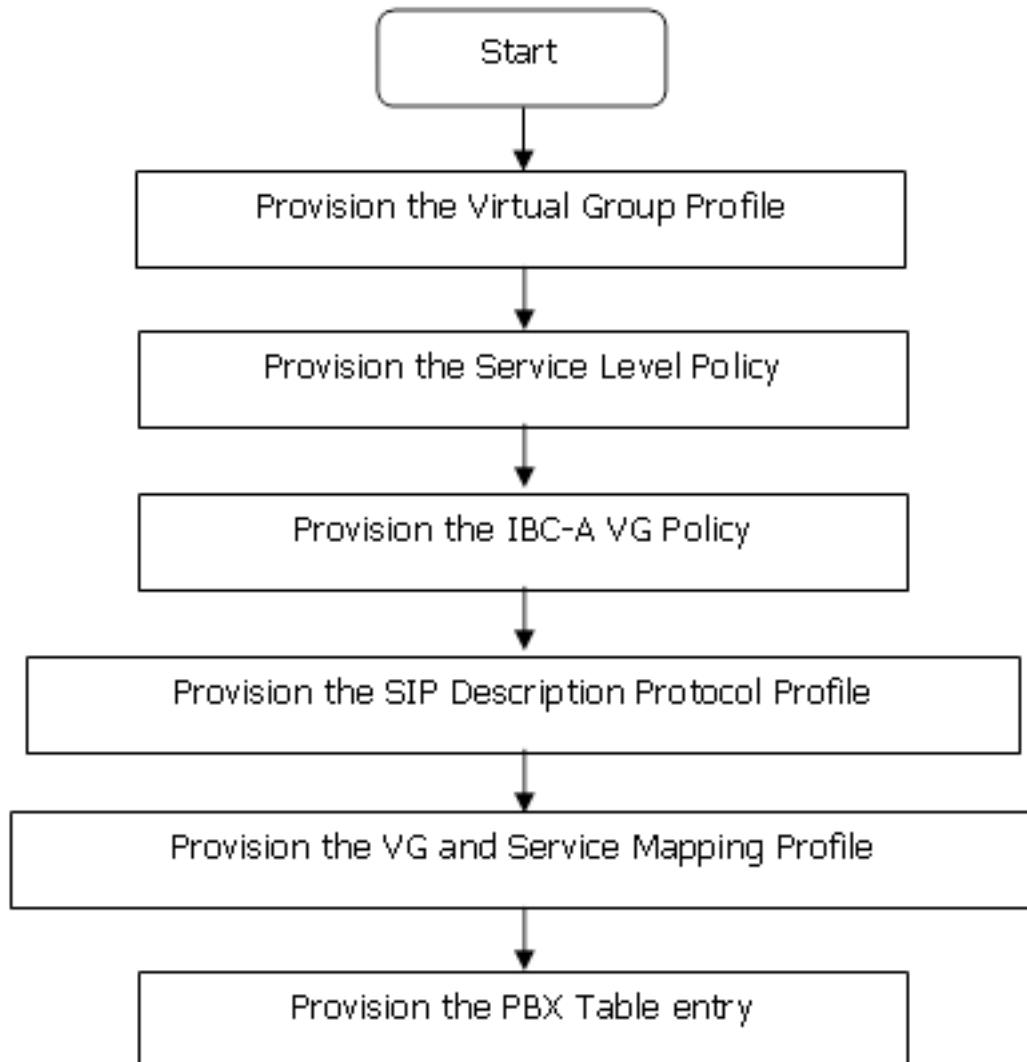
---

**10 Add PDP Port to IMS Service**

See “[To provision a Diameter port](#)” (p. 10-108)

**Virtual Group task flow diagram**

It is optional to provision the Virtual Group.



## Virtual Group Task flow

### 1 Provision the Virtual Group Profile

Configure “Virtual Group Member” in virtual group profile. Session admission control and IBC route profile selection may be applied on this “virtual group member”.

See “[To provision a Virtual Group profile](#)” (p. 5-125)

### 2 Provision the Service Level Policy

Configure “session count” and “bandwidth”@gamil policy.

See “[To provision a Service Level Policy](#)” (p. 5-129)

### 3 Provision the IBC-A VG Policy

Configure the routing policy for one virtual group.

See “[To provision the IBC-A VG Policy](#)” (p. 5-133)

### 4 Provision the SIP Description Protocol Profile

See “[To provision a Session Description Protocol Profile](#)” (p. 4-62)

### 5 Provision the VG and Service Mapping Profile

Associate above defined:

- Service Level Policy (virtual group profile)
- IBC-A Virtual Group Policy (IBC-A VG Policy)
- SDP Policy (SIP Description Protocol Profile)

See “[To provision a VG and Service Mapping Profile](#)” (p. 5-137)

## Surrogate Registration for PBX Gateway task flow diagram

Provision the PBX Table entry

- Configure the REGISTER information for one PBX in PBX table entry
- Associate PBX Table in SIPia Port

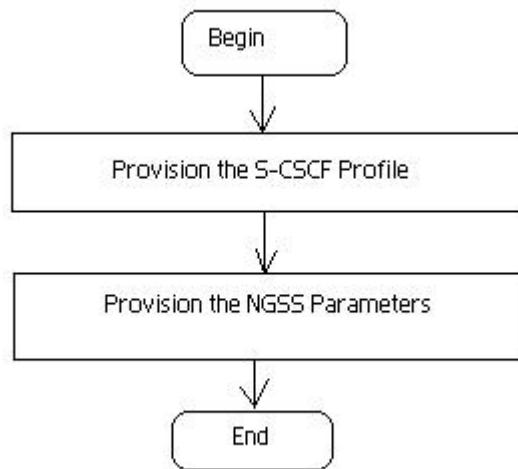
See: “[To provision PBX Table Entry](#)” (p. 4-96)

# Provisioning Task flow - To provision S-CSCF Assisted Relocation Procedure for Geo-Redundancy Enhancement

## Purpose

This provisioning task flow provides the steps to provision S-CSCF Assisted Relocation Procedure for Geo-Redundancy Enhancement.

## Provisioning task flow diagram



## Steps to provision S-CSCF Assisted Relocation Procedure for Geo-Redundancy Enhancement

Perform the following steps:

### 1 Provision the S-CSCF Profile.

Enable the **Send immediate dereg SAR for unregistered call** check box.

See “[To provision an S-CSCF profile](#)” (p. 4-15) for more information.

### 2 Provision the NGSS Parameters.

Provision the following parameters:

- **S-CSCF relocation for geo-redundancy**
- **Minimum duration of registry before relocation attempt**

See “[To provision NGSS Server parameters](#)” (p. 10-9) for more information.

# Provisioning Task flow - To provision iAGCF Line OOS and CPC Display functionalities

## Overview

This topic provides the steps to provision the following iAGCF functionalities:

- iAGCF Line OOS
- CPC Display

### iAGCF Line OOS - Provisioning task flow

#### 1 Provision the AGCF Profile.

Provision the following parameters under the **Line OOS - Channel Parked** group box:

- **SIP Response Code** - This parameter controls which SIP error code to use in a response to an attempted call termination to an iAGCF user in the parked state.
- **Include Reason Header** - This parameter controls whether the iAGCF includes the following specific Reason header in SIP error responses to attempted call terminations to an iAGCF user in the parked state: Reason: Q.850 ;cause=27 ;text=" Destination Out of Service"

See *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420, for more information.

#### 2 Provision the AGCF Gateway Variant.

Provision the **Silence between Cause Code Tones** parameter- This parameter controls whether the iAGCF inserts a period of silence between the 1st and 2nd tones provisioned as part of the "No Digit Match" condition in the "iAGCF cause code to H.248 Tone mapping" table.

The value is used only if the second tone for the treatment is 'reduced battery'.

See *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420, for more information.

### CPC Display - Provisioning task flow

#### 1 Provision the AGCF CPC String to CPC Digit Table.

See “[To provision an AGCF CPC String to CPC Digit Table](#)” (p. 5-328) for more information.

**2** Provision the AGCF Profile.

Provision the following parameter under the **CPC Parameters** group box:

- **Include CPC Digit in Caller ID** - This parameter controls whether the terminating iAGCF includes a CPC digit in the Caller ID.

**Note:** If the **Include CPC Digit in Caller ID** check box is checked, at least one record must exist in the CPC String to CPC Digit table.

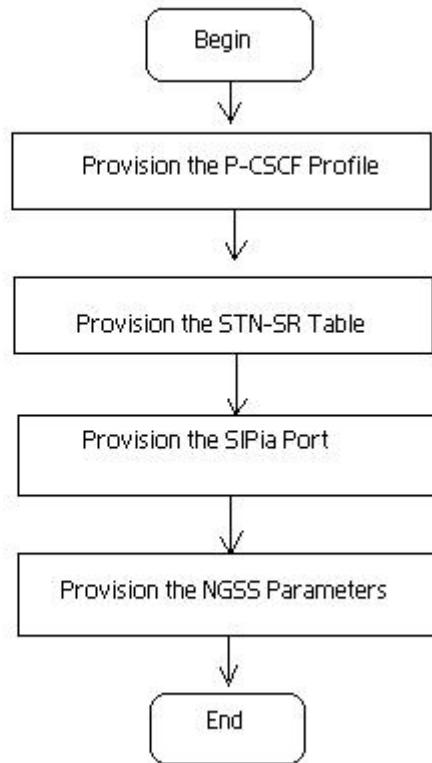
See *1310 OMC-P for Alcatel-Lucent Control Platform User Guide for Managing the 5420 Converged Telephony Server (CTS) and the 5450 IP Session Control (ISC)*, 255-400-420, for more information.

# To provision ATCF support

## Purpose

This provisioning task flow provides the steps for provisioning support of ATCF functionality.

## Provisioning task flow diagram



## Steps to provision ATCF support functionality

Perform the following steps:

---

1 Provision the P-CSCF profile

On the **ATCF Configuration Parameters** tab of the P-CSCF Profile, provision the following parameters:

- **Support ATCF**
- **Policy to Include ATCF**

- **Policy to Include ATGW**
- **Policy for Media Transcoding During eSRVCC**
- **Wait for Possible eSRVCC Before Call Clearing Timer**
- **Send ACR For HO Request**
- **Send BYE to UE to Release Source Access Leg**

See “[To provision PCSCF profile](#)” (p. 4-77) for more information.

---

**2** Provision the STN-SR table

See “[To provision an STN-SR Table](#)” (p. 5-332) for more information.

---

**3** Provision the SIPia port

Select the appropriate option from the **STN-SR ID** list.

See “[To provision a SIPia port](#)” (p. 10-40) for more information.

---

**4** Provision the NGSS Parameters

Select the appropriate option from the **MSC Core Realm Id** list.

See “[To provision NGSS Server parameters](#)” (p. 10-9) for more information.

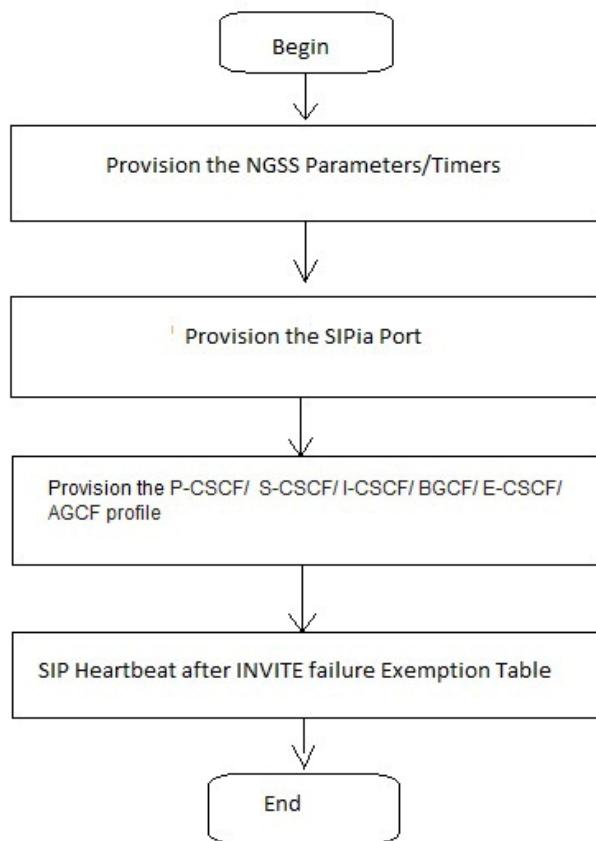
# Provisioning Task flow - To provision SIP heartbeat after failure to reach a network element

## Purpose

This provisioning task flow provides the steps to provision SIP heartbeat after failure to reach a network element.

## Provisioning task flow diagram

The following figure illustrates the provisioning task flow for provisioning the SIP heartbeat after failure to reach a network element.



## Steps to provision SIP heartbeat after failure to reach a network element

Perform the following steps:

---

**1 Provision NGSS Parameters/Timers.**

Provision the parameter, **Support SIP Heartbeat after failure** in the NGSS Parameters/Timers window.

See “[To provision NGSS Server parameters](#)” (p. 10-9) for more information.

---

**2 Provision a SIPia Port.**

Provision the parameter, **Support SIP Heartbeat after failure** in the SIPia Port Configuration window.

See “[To provision a SIPia port](#)” (p. 10-40) for more information.

---

**3 Provision the desired P-CSCF/ S-CSCF/ I-CSCF/ BGCF/ E-CSCF/ AGCF component.**

For example,

Provision a P-CSCF Profile.

Provision the parameter, **SIP Heartbeat after failure on Gm Interface** in the P-CSCF Profile window.

See “[To provision PCSCF profile](#)” (p. 4-77) for more information.

---

**4 Provision a SIP Heartbeat after failure Exemption Table.**

Provision the following parameters:

- **Entry ID**
- **Destination Address Type**
- **Destination**
- **Port Number**
- **Transport**

See “[To provision an SIP Heartbeat after failure Exemption Table](#)” (p. 5-337) for more information.

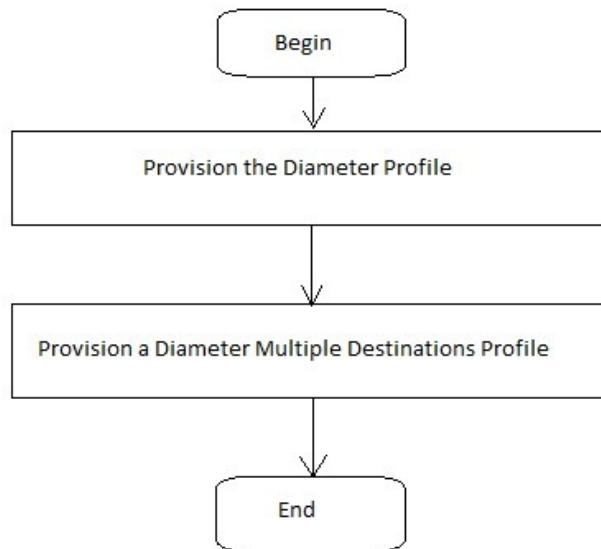
# Provisioning task flow - To provision primary and alternate SLF destination for geo-redundancy support

## Purpose

This provisioning task flow provides the steps to provision primary and alternate SLF destination for geo-redundancy support .

## Provisioning task flow diagram

The following figure illustrates the provisioning task flow for provisioning the primary and alternate SLF destination for geo-redundancy support functionality.



---

## Steps to provision primary and alternate SLF destination for geo-redundancy support

Perform the following steps:

---

**1 Provision the Diameter Profile.**

Provision the parameter **Min Percentage of Active Agent/Backup Connections** on the Diameter Connection Interface Configuration Screen (in Diameter Profile).

See “[To provision a Diameter profile](#)” (p. 10-23).

**Note:** This functionality is only supported for all diameter interfaces on Client. The **Min Percentage of Active Agent/Backup Connections** is only applicable for Diameter Multiple Destinations Profile. This field is grayed out when no Multiple Destinations profile is provisioned.

---

**2 Provision a Diameter Multiple Destinations Profile.**

Provision the parameter **Geo-Redundancy Type** on the Diameter Multiple Destinations Profile Configuration Screen.

See “[To provision a Diameter Multiple Destination Profile](#)” (p. 4-278).

**Notes:**

- All the FQDNs in the Multiple Destinations FQDN list can be checked as Primary (Agent or Backup) FQDN.
- One or more FQDNs provisioned in the multiple FQDN list can be checked as Alternate Agent FQDN if at least one Primary Agent FQDN is checked.
- One or more FQDNs provisioned in the multiple FQDN list can be checked as Alternate Backup FQDN if at least one Primary Backup FQDN is checked.
- If both Agent and Backup are disabled, **Geo-Redundancy Type** can only be set to “None”.
- It is not allowed to set both “Agent” and “Backup” to Yes at the same time.
- **Geo-Redundancy Type** cannot be “None” if Agent or Backup FQDN is enabled.

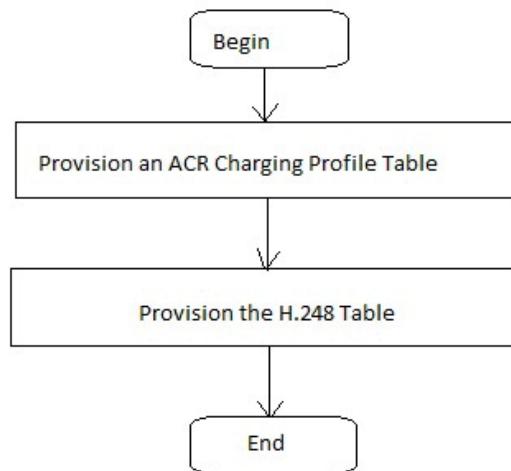
# Provisioning Task flow - To support new versions of IMS charging SPEC 3GPP 32.260

## Purpose

This provisioning task flow provides the steps to provision support for new versions of IMS charging SPEC 3GPP 32.260. In other words, this task flow describes the provisioning process to support V9 and higher version ACR.

## Provisioning task flow diagram

The following figure illustrates the provisioning task flow for provisioning support for new versions of IMS charging SPEC 3GPP 32.260.



---

## Steps to provision support for new versions of IMS charging SPEC 3GPP 32.260

Perform the following steps in order to support V9 and higher version ACR:

---

**1** Provision an ACR Charging Profile.

Provision the following parameters:

- **Release Number**
- **Extension Number**

See “[To provision an ACR Charging Profile](#)” (p. 8-5).

---

**2** Provision the H.248 Table.

Provision the parameter, **ACR Charging Profile Id** in the H.248 Table.

See “[To add an H.248 Device Server](#)” (p. 7-29).

# 2 SPDF

## Overview

### Purpose

This chapter provides the provisioning task flows to configure the Service Policy Decision Function (SPDF) -3GPP2 SBBC and TISPAN RACS.

### Contents

|  |            |
|--|------------|
| <b>3GPP2 SBBC</b>                          | <b>2-2</b> |
| 3GPP2 SBBC provisioning task flow          | 2-3        |
| PD-FE 3GPP2 policy provisioning task flow  | 2-6        |
| <b>TISPAN RACS</b>                         | <b>2-8</b> |
| TISPAN RACS provisioning task flow         | 2-9        |
| PD-FE TISPAN policy provisioning task flow | 2-15       |
| Media Inactivity provisioning task flow    | 2-16       |

# 3GPP2 SBBC

## Overview

### Purpose

This section provides the task flows to configure 3GPP2 SBBC.

### Contents

|   |     |
|---|-----|
| <a href="#">3GPP2 SBBC provisioning task flow</a>         | 2-3 |
| <a href="#">PD-FE 3GPP2 policy provisioning task flow</a> | 2-6 |

# 3GPP2 SBBC provisioning task flow

## Purpose

This topic provides the provisioning task flow for 3GPP2 SBBC.

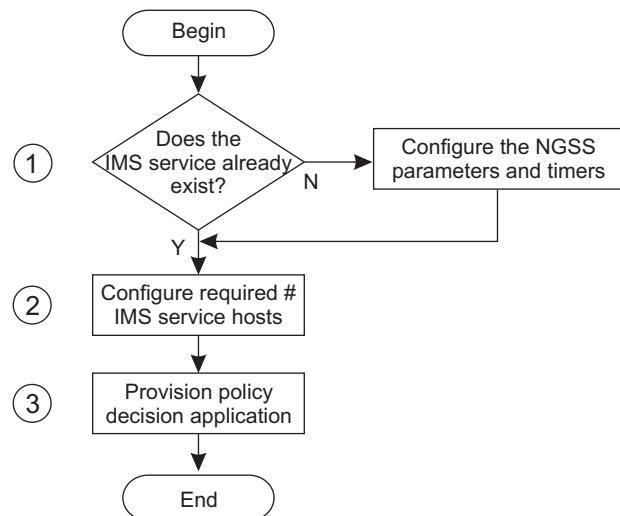
## Before you begin

This task flow assumes the IMS service and NGSS Server parameters are already configured.

See “[To provision an IMS Service association](#)” (p. 10-20).

## Flow diagram

The flow diagram:



## 3GPP2 SBBC provisioning tasks

Perform the following stages:

- 1 Provision Diameter Application IDs.

The Diameter Application IDs define the interfaces between Diameter servers and Diameter clients.

The following table shows the applications IDs that you must provision:

| Technology | Interfaces      |
|------------|-----------------|
| 3GPP2      | Sp'<br>Tx<br>Ty |

See “[To modify Diameter application IDs](#)” (p. 10-31).

**2** Provision a Diameter profile.

Diameter profile provisioning includes provisioning Diameter connection interfaces.

Define a Profile ID and a Profile Name and enter the following values.

| Standards | Parameter                            | Value |
|-----------|--------------------------------------|-------|
| 3GPP2     | <b>Diameter Connection Interface</b> | Sp'   |

See “[To provision a Diameter profile](#)” (p. 10-23).

**3** Provision a service to Diameter mapping.

See “[To provision a Service to Diameter mapping](#)” (p. 10-32).

**4** Provision the PD-FE-related policy tables.

See “[PD-FE 3GPP2 policy provisioning task flow](#)” (p. 2-6).

**5** Provision the PDF profile for 3GPP2.

1. Select **3GPP2** as **Diameter Interface Type**
2. Configure a **Service Indication**
3. Configure other parameters as required.

For the other parameters, the default values can be used.

See “[To provision a PDF profile](#)” (p. 10-104).

**6** Provision a PD-FE port on the IMS service.

Assign the PDF profile you created to the PD-FE port.

---

See “To provision a Diameter port” (p. 10-108).

# PD-FE 3GPP2 policy provisioning task flow

## Purpose

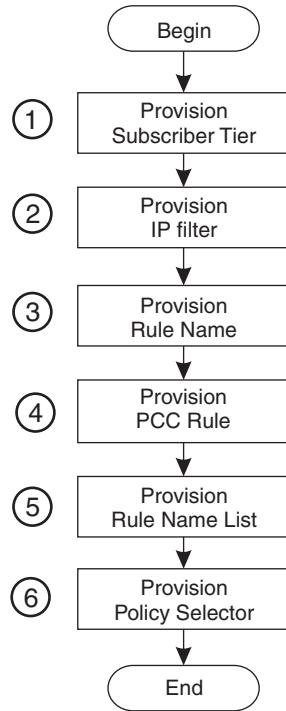
This topic provides the provisioning task flow to provision a PD-FE policy for 3GPP2.

## Before you begin

Observe the following:

- Using the FS GUI *System View*, a redundant pair of hosts must already have been associated with the IMS service.

## Provisioning taskflow diagram



## PD-FE Policy provisioning tasks

Perform the following steps to provision an S-CSCF:

- 
- 1 Provision the Subscriber Tier table to store the subscriber tiers. See: “[To provision a Subscriber Tier table](#)” (p. 7-3).

- 
- 2 Provision the IP Filter table to store the IP filters. See: “[To provision an IP Filter table](#)” (p. 7-6).

---

  - 3 Provision the Rule Name table to store the rule names that are used to form charging rules. See: “[To provision a Rule Name table](#)” (p. 7-11).

---

  - 4 Provision the PCC Rule table to store the PCC rules used to form charging rules. See: “[To provision a PCC Rule table](#)” (p. 7-14).

---

  - 5 Provision the Rule Name List table to store the rule name lists used to form charging rules. See: “[To provision a Rule Name List table](#)” (p. 7-20).

---

  - 6 Provision the Policy Selector used to search for policy rules. See: “[To provision a Policy Selector Table](#)” (p. 7-24).

# TISPAN RACS

## Overview

### Purpose

This section provides the task flows to configure the TISPAN RACS.

### Contents

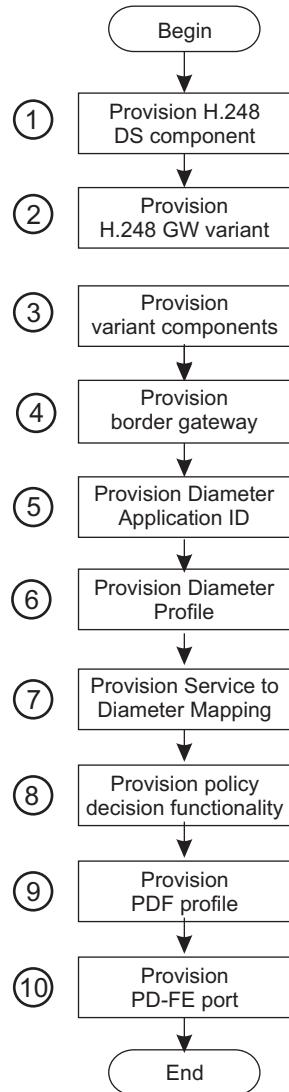
|  |      |
|--|------|
| TISPAN RACS provisioning task flow         | 2-9  |
| PD-FE TISPAN policy provisioning task flow | 2-15 |
| Media Inactivity provisioning task flow    | 2-16 |

# TISPAN RACS provisioning task flow

## Purpose

This topic provides the provisioning task flow for a TISPAN RACS.

## Provisioning taskflow diagram



## Before you begin

This task flow assumes the IMS service and NGSS Server parameters are already configured.

Refer to “[To provision an IMS Service association](#)” (p. 10-20).

## TISPA N RACS provisioning tasks

Perform the following stages:

- 1 Provision an H.248 DS component.

**Reference:** Refer to “[To add an H.248 Device Server](#)” (p. 7-29).

- 2 Provision an H.248 GW variant. The H.248 GW variant will be used by the BGC.

**Reference:** Refer to “[To provision a variant](#)” (p. 10-114).

- 3 Provision the components for the H.248 GW variant that is used by the BGC.

The following table shows the recommended values for the variant:

| <b>Id</b> | <b>Parameter</b>                      | <b>Recommended value</b> |
|-----------|---------------------------------------|--------------------------|
| 000       | Long Timer                            | 30000                    |
| 001       | MaxNoOfContexts                       | 16000                    |
| 002       | MaxNoOfRetransmissions                | 2                        |
| 003       | MaxNoOfTerminalsPerContext            | 2                        |
| 004       | ReTxTimerExponential                  | N                        |
| 005       | ReTxTimerOnTransPending               | 1500                     |
| 006       | RxTxTimer                             | 1500                     |
| 007       | HBTimer                               | 1500                     |
| 008       | MaxHBRetransmission                   | 4                        |
| 009       | Maximum Inactivity Time               | 3000                     |
| 010       | Dynamic Payload for Clear Mode        | N                        |
| 011       | IP Interworking Support (Y/N)         | N                        |
| 012       | Congestion Handling Support           | Y                        |
| 013       | Media Negotiation Support             | N                        |
| 014       | Use TDM Sub-Prefix (Y/N)              | N                        |
| 015       | Number of Audit Value Per Transaction | 5                        |
| 016       | Sequential Signal List Supported      | N                        |

| <b>Id</b> | <b>Parameter</b>   | <b>Recommended value</b>   |
|-----------|--|--|
| 017       | TDM-TDM Hairpin Active   | N (default value)  |
| 018       | Hang Term Active (Y/N)   | N  |
| 019       | Hang Term Timer Value  | 0, if the BGW has a provisioned default value for Hang Term timers.<br>About 3 x the average hold time of a call in the network (in seconds) |
| 020       | H.248.11 Congestion Handling Support Via H.248.11  | Y/N  |
| 021       | H.248.11 MaxFill – Number of Tokens at which bucket is full. (Range 1 – 32000.)                                | 5000   |
| 022       | H.248.11 InitialFill – Initial number of tokens present. (Range 1 – 32000.)                                    | 2500   |
| 023       | H.248.11 LeakInterval – Timer to Schedule the removal of Tokens. (Range 100ms – 10000ms.)                      | 1000   |
| 024       | H.248.11 InitialLeakAmount – Initial Value of Leak Amount (Range 1 – 32000.)                                   | 5000   |
| 025       | H.248.11 TargetOverloadRate – Rate of Overload notifications. (Range 1m – 60m.)                                | 30m  |
| 026       | H.248.11 OverloadSamplingInterval – Timer to check the number of overload notifications. (Range 1sec – 30sec.) | 10sec  |
| 027       | H.248.11 TerminationPendingPeriod – Timer to remove the Control. ( Range 1m – 10 m.)                           | 2m   |
| 028       | QoS Statistics (Y/N)   | N  |
| 029       | IPDC Support via H.248.41 (Y/N)  | N  |
| 030       | No Bypass of Router (Y/N)  | N  |
| 031       | Application data inactivity detection package via H.248.40 (Y/N)   | N  |
| 032       | Spare1(Y/N)  | N  |
| 033       | Spare2   | 0  |

| <b>Id</b> | <b>Parameter</b> | <b>Recommended value</b> |
|-----------|------------------|--------------------------|
| 034       | Spare3           | 0                        |
| 035       | Spare4           | 0                        |

**Reference:** Refer to “To provision a PPL component in a signaling variant” (p. 10-116).

**4** Provision the border gateway.

**Reference:** Refer to “To provision an H.248-controlled BGW” (p. 7-32).

**5** Provision a Diameter Application ID.

The following table shows the Diameter Application IDs that are required:

| <b>Standard</b> | <b>Diameter Application Interface/IDs</b> |
|-----------------|---|
| TISPA           | Gq'                                       |
|                 | Rw'                                       |
|                 | Rq (optional)                             |
|                 | Rf (optional)                             |

**Reference:** Refer to “To modify Diameter application IDs” (p. 10-31).

**6** Provision a Diameter Profile table.

Diameter profile provisioning includes provisioning Diameter connection interfaces.

Define a Profile ID and a Profile Name and enter the following values.

| <b>Standards</b> | <b>Parameter</b>                              | <b>Value</b>                            |
|------------------|---|---|
| TISPA            | <b>Diameter Connection Interface</b>          | Rw'<br>Rf (optional for QoS Statistics) |
|                  | <b>Min Percentage of Active Connections %</b> | 100<br>(for Rw')<br>50<br>(for Rf)      |

**Reference:** Refer to “To provision a Diameter profile” (p. 10-23).

**7** Provision the Service to Diameter Mapping Table.

|        | Parameter    | Value                                 |
|--------|--------------|---------------------------------------|
| TISPAN | Service Type | H.248                                 |
|        | Blade        | Select the H.248 DS that acts as BGC. |

**Reference:** Refer to “To provision a Service to Diameter mapping” (p. 10-32).

**8** **When ...** **Then ...**

|                                       |   |
|---------------------------------------|---|
| you want to provision a TISPAN PD-FE, | Provision the TISPAN PD-FE policy.<br>Refer to “PD-FE TISPAN policy provisioning task flow” (p. 2-15) |
|---------------------------------------|---|

**9** Provision the PDF Profile table.

| When ...                                    | Then ...  |
|---|---|
| you want to provision a TISPAN PDF profile, | <ol style="list-style-type: none"> <li>1. Select <b>TISPAN</b> as <b>Diameter Interface Type</b></li> <li>2. Select a <b>DSCH Profile ID</b></li> <li>3. Configure other parameters as required.<br/>For the other parameters, the default values can be used.</li> </ol> |

Refer to “To provision a PDF profile” (p. 10-104).

**10** Provision a PD-FE port on the IMS service.

Assign the PDF profile you created to the PD-FE port.

Refer to “To provision a Diameter port” (p. 10-108).

**11** Provision a H.248 Device Server

Select the proper ACR version based on the capabilities of the CCF.

---

Refer to “To add an H.248 Device Server” (p. 7-29)

# PD-FE TISPAN policy provisioning task flow

## Purpose

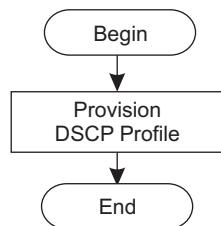
This topic provides the provisioning task flow to provision a PD-FE policy for TISPAN RACS.

## Before you begin

Observe the following:

- Using the FS GUI *System View*, a redundant pair of hosts must already have been associated with the IMS service.

## Provisioning taskflow diagram



## Provisioning task

Perform the following:

- 
- 1 Provision a DSCP profile table.

Refer to “[To provision a DSCP Profile table](#)” (p. 7-36).

# Media Inactivity provisioning task flow

## Purpose

This topic describes the provisioning task flow for Media Inactivity.

## Provisioning task flow

Perform the following steps:

---

**1** Provision the NGSS Parameters/Timers Screen.

Provision the following parameters on the **NGSS Parameters/Timers** Screen:

- **Audio Media Inactivity Timer**
- **Video Media Inactivity Timer**
- **Message Media Inactivity Timer**
- **Other Media Inactivity Timer**

Refer, “[To provision NGSS Server parameters](#)” (p. 10-9).

---

**2** Provision the H.248 Gateway Variant Screen.

On the **H.248 Gateway Variant** screen provision the parameter **Application data inactivity detection package via H.248.40**.

Refer, “[TISPAN RACS provisioning task flow](#)” (p. 2-9).

# 3 Offline charging

## Overview

### Purpose

This chapter provides the task flows to perform offline charging-related accounting management tasks.

### Contents

|   |            |
|---|------------|
| <b>ACR and ABF provisioning task flows</b>          | <b>3-2</b> |
| Provision ACR task flow                             | 3-3        |
| ACR Buffering Function (ABF) provisioning task flow | 3-5        |

# ACR and ABF provisioning task flows

## Overview

### Purpose

This section provides the task flows to provision the ACR and the ACR Buffering Function (ABF).

### Contents

|   |     |
|---|-----|
| <a href="#">Provision ACR task flow</a>                             | 3-3 |
| <a href="#">ACR Buffering Function (ABF) provisioning task flow</a> | 3-5 |

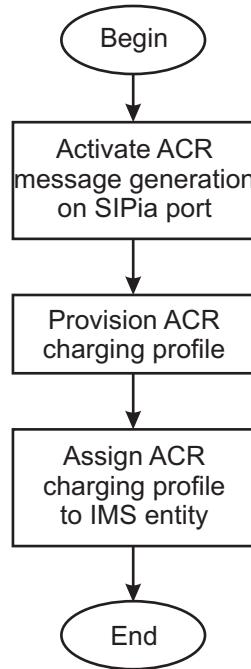
# Provision ACR task flow

## Purpose

This topic describes the task flow to provision ACR.

## ACR provisioning task flow

The following figure shows the task flow to provision ACR:



## ACR provisioning task flow stages

- 1 Activate ACR message generation on the SIPia port.

**Reference:** Refer to “To activate an ACR message generation on a SIPia port” (p. 8-3)

- 2 Provision an ACR charging profile.

The ACR charging profile defines when ACR messages are generated.

**Reference:** Refer to “[To provision an ACR Charging Profile](#)” (p. 8-5).

- 
- 3 Assign an ACR charging profile to the IMS entity.

Assigning an ACR charging profile provides additional control about when ACR messages are generated. When no profile is assigned, the default options are used.

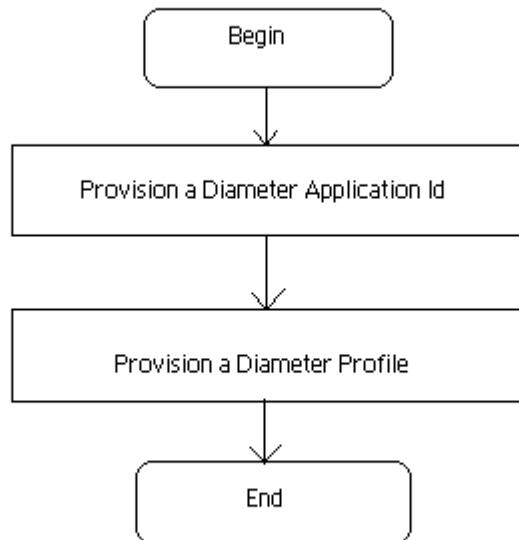
**Reference:** Refer to “[Assigning an ACR Charging profile to an IMS entity](#)” (p. 8-15).

# ACR Buffering Function (ABF) provisioning task flow

## Purpose

This topic provides the task flow that should be followed to provision the ACR Buffering Function (ABF).

## Provisioning ABF taskflow



## Provisioning ABF

Perform the following steps to provision the ABF.

---

### 1 Provision the Diameter Application Id.

Configure the Diameter Application ID for the ABF interface. The default value of the Diameter Application ID for the ABF interface is 3.

Configure the following parameters:

| Parameter | Value |
|-----------|-------|
| ABF       | 3     |

Refer to “[To modify Diameter application IDs](#)” (p. 10-31).

---

**2** Provision the Diameter Profile.

Refer to “[To provision an ABF Diameter profile table](#)” (p. 8-24).

# Part II: IP session control (ISC) configuration

## Overview

### Purpose

This part of the documentation describes Configuration Management concepts and provides procedures to users to perform Configuration Management tasks related to the IP Session Control (ISC).

### Contents

|  |     |
|--|-----|
| Chapter 4, Manage system configuration | 4-1 |
| Chapter 5, Manage services             | 5-1 |
| Chapter 6, Translations                | 6-1 |



# 4 Manage system configuration

## Overview

### Purpose

This chapter provides the procedures to configure the parameters/timers related to the IMS Server and the IMS components part of the Alcatel-Lucent IP Session Control.

### Contents

|   |             |
|---|-------------|
| <b>S-CSCF provisioning</b>                                  | <b>4-5</b>  |
| To provision SDP media                                      | 4-6         |
| To provision an S-CSCF profile                              | 4-15        |
| To provision Emergency Session Routing Method               | 4-26        |
| To provision support for wildcard PUID                      | 4-27        |
| To activate PacketCable authentication in an S-CSCF profile | 4-29        |
| To provision a S-CSCF PSI URI table                         | 4-31        |
| To provision a Home Network Identifier profile table        | 4-33        |
| To activate enhanced third party registration               | 4-35        |
| To provision the S-CSCF profile to support IP-PBX calls     | 4-36        |
| Provisioning Task flow - To provision S-CSCF pool           | 4-40        |
| <b>I-CSCF provisioning</b>                                  | <b>4-44</b> |
| To provision ICSCF Profile                                  | 4-45        |
| To provision the S-Cscf Capability List                     | 4-53        |
| To create a PSI sub-domain list                             | 4-57        |
| <b>P-CSCF provisioning</b>                                  | <b>4-61</b> |
| To provision a Session Description Protocol Profile         | 4-62        |
| To provision Service-Based PCSCF Profile                    | 4-69        |

|  |              |
|--|--------------|
| To provision SIP Stack Timer Profile                         | 4-74         |
| To provision PCSCF profile                                   | 4-77         |
| To provision PBX Table Entry                                 | 4-96         |
| To activate the SIP header reduction                         | 4-101        |
| To activate Service Route header                             | 4-102        |
| To activate PacketCable authentication in the P-CSCF profile | 4-104        |
| To provision SIP compression                                 | 4-106        |
| To provision IMS Signaling security                          | 4-108        |
| To provision the Service Based Local Policy Profile          | 4-111        |
| To provision e2 interface support                            | 4-116        |
| Support to provide P-CSCF IP address to UE                   | 4-120        |
| To provision the TLS Profile table                           | 4-121        |
| To provision the SIP Error Treatment Table attributes        | 4-123        |
| Provisioning Task flow - To provision P-CSCF pool            | 4-126        |
| <b>BGCF provisioning</b>                                     | <b>4-132</b> |
| To provision BGCF URI Id                                     | 4-133        |
| To provision BGCF Target List                                | 4-138        |
| To provision BGCF Profile                                    | 4-142        |
| To provision BGCF Time Of Day                                | 4-148        |
| To provision BGCF Network Gateway                            | 4-152        |
| To provision BGCF Default Network Gateway                    | 4-156        |
| To provision Originating Host Class Profile routing for BGCF | 4-160        |
| To provision Subscriber Profile routing for BGCF             | 4-163        |
| To provision BGCF DA Route Table                             | 4-172        |
| To provision BGCF SIP content type                           | 4-177        |
| To provision BGCF local number routing                       | 4-181        |
| To provision BGCF location based routing                     | 4-189        |
| To provision BGCF Originating Host ID                        | 4-193        |
| <b>IBCF provisioning</b>                                     | <b>4-197</b> |
| To provision IBCF Profile                                    | 4-198        |
| <b>E-CSCF provisioning</b>                                   | <b>4-204</b> |
| Emergency provisioning scenarios                             | 4-205        |
| To provision IMS Emergency Service Identifier                | 4-208        |

|  |              |
|--|--------------|
| To provision an E-CSCF Profile table                                     | 4-212        |
| <b>NTM provisioning</b>  | <b>4-221</b> |
| To provision an NTM Control table  | 4-222        |
| To provision an NTM Exemption table                                      | 4-226        |
| To provision an I-CSCF profile table                                     | 4-230        |
| <b>EEAS provisioning</b>   | <b>4-237</b> |
| To provision an E.164 Expansion AS profile                               | 4-238        |
| <b>IMS gateway function provisioning</b>                                 | <b>4-241</b> |
| To provision Online Charging Trigger Data table                          | 4-242        |
| To provision MRF Announcement Interface profile                          | 4-245        |
| To provision MRF Announcement Data table                                 | 4-247        |
| To provision IGWF profile  | 4-250        |
| <b>P-NAPTR provisioning</b>  | <b>4-252</b> |
| To provision a P-NAPTR Region  | 4-253        |
| To provision a P-NAPTR Target URI  | 4-257        |
| <b>iAGCF provisioning</b>  | <b>4-260</b> |
| Introduction to the base configuration                                   | 4-261        |
| <b>SIP permanent linksets provisioning</b>                               | <b>4-263</b> |
| To provision an SIP Linkset  | 4-264        |
| To provision an SIP Permanent Linkset Group                              | 4-269        |
| <b>Provisioning diameter multiple destination FQDNs</b>                  | <b>4-272</b> |
| Conversion from Diameter Geo-redundancy to support Multiple destinations | 4-273        |
| Conversion from Multiple destination to support Diameter Geo-redundancy  | 4-276        |
| To provision a Diameter Multiple Destination Profile                     | 4-278        |
| <b>Border gateway provisioning</b>                                       | <b>4-282</b> |
| To provision a Core Bearer Realm   | 4-283        |
| To provision a Published Realm   | 4-286        |
| To assign a Published Realm to a Border Gateway                          | 4-290        |
| <b>Central Routing Function provisioning</b>                             | <b>4-293</b> |
| CRF provisioning task flow   | 4-294        |
| To provision a CRF Target table  | 4-297        |
| To provision a CRF Target List table                                     | 4-302        |
| To provision a CRF Treatment table                                       | 4-306        |

|  |       |
|--|-------|
| To provision a CRF Digit Analysis Table      | 4-310 |
| To provision a CRF Trunk Group table         | 4-313 |
| To provision a CRF Route Plan table          | 4-316 |
| To provision a CRF Task Plan table           | 4-320 |
| To provision a CRF Route Priority List table | 4-324 |
| To provision a CRF Route Profile table       | 4-328 |

# S-CSCF provisioning

## Overview

### Purpose

This section provides the procedures that are used to provision the Serving CSCF (S-CSCF).

### Contents

|   |      |
|---|------|
| To provision SDP media                                      | 4-6  |
| To provision an S-CSCF profile                              | 4-15 |
| To provision Emergency Session Routing Method               | 4-26 |
| To provision support for wildcard PUID                      | 4-27 |
| To activate PacketCable authentication in an S-CSCF profile | 4-29 |
| To provision a S-CSCF PSI URI table                         | 4-31 |
| To provision a Home Network Identifier profile table        | 4-33 |
| To activate enhanced third party registration               | 4-35 |
| To provision the S-CSCF profile to support IP-PBX calls     | 4-36 |
| Provisioning Task flow - To provision S-CSCF pool           | 4-40 |

# To provision SDP media

## Purpose

This procedure is used to provision Session Description Protocol (SDP) media.

The procedure provides the steps to provision the following SDP media information:

- SDP media codec
- SDP media component policy
- SDP media subscription profile
- SDP Media MSRP table

The SDP media provisioning is performed in the S-CSCF.

**Important!** If both SDP media subscription validation and SDP local policy validation apply, the S-CSCF validates only SDP media subscription.

## Steps to provision a SDP media codec table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → SCSCF Tables**.

**Result:** The **SCSCF Tables** window is displayed.

- 2 In the left pane, expand the **SDP Media Codec** folder.

**Result:** The SDP Media Codec tables are listed under the folder in the left pane.

If the folder is empty, add a SDP media codec table.

Perform the following steps in the **SCSCF Tables - SDP Media Codec** window to add, rename, or delete a SDP media codec table :

| If you want to ...           | then ...  |
|------------------------------|---|
| add a SDP media codec table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add SDP Media Codec table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.<br/><i>End of steps</i></li> </ol> |

| If you want to ...              | then ...  |
|---------------------------------|---|
| rename a SDP media codec table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename SDP Media Codec table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a SDP media codec table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a SDP media codec table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>                  |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the SDP media codec table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **SCSCF Tables - SDP Media Codec** window to add, modify, or delete the SDP media codec table attributes:

| If you want to ...                        | then ...   |
|---|--|
| add the SDP media codec table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SDP Media Codec</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                         | then ...   |
|--|--|
| modify a SDP media codec table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SDP Media Codec</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol> |
| delete a SDP media codec table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.<br/><i>End of steps.</i></li> </ol>                   |

**5** Provision the following parameters:

| Parameter         | Provisioning                                      |
|-------------------|---|
| <b>Codec ID</b>   | Select a unique ID for the SDP Media Codec table. |
| <b>Name</b>       | Type a descriptive name for the SDP Media Codec.  |
| <b>Codec Type</b> | Select the Codec Type                             |
| <b>Parameter</b>  | Provision the Codec parameters                    |

For more information on the parameters, see the topic **SDP Media Codec** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

**6** Click **OK**.

**Result:** The SDP media codec table attributes are provisioned successfully.

END OF STEPS

## Steps to provision an SDP media component policy table

Perform the following steps at the Provisioning GUI:

- 1 Select IMS → IMS Components → SCSCF Tables.

**Result:** The SCSCF Tables window is displayed.

- 2 In the left pane, expand the SDP Media Component Policy folder.

**Result:** The SDP Media Component Policy tables are listed under the folder in the left pane.

If the folder is empty, add a SDP Media Component Policy table.

Perform the following steps in the SCSCF Tables - SDP Media Component Policy window to add, rename, or delete a SDP Media Component Policy table :

| If you want to ...                         | then ...  |
|--|---|
| add a SDP Media Component Policy table,    | <ol style="list-style-type: none"><li>1. Select Tables → Add Table.<br/><b>Result:</b> The Add SDP Media Component Policy table window is displayed.</li><li>2. From the Table Number list, select the table number.</li><li>3. In the Table Name box, type a descriptive table name.</li><li>4. Click OK.</li></ol> <p><i>End of steps</i></p> |
| rename a SDP Media Component Policy table, | <ol style="list-style-type: none"><li>1. Select the table, and then select Tables → Rename table.<br/><b>Result:</b> The Rename SDP Media Component Policy table window is displayed.</li><li>2. In the Table Name box, type a new table name.</li><li>3. Click OK.</li></ol> <p><i>End of steps</i></p>  |

| If you want to ...                         | then ...  |
|--|---|
| delete a SDP Media Component Policy table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a SDP Media Component Policy table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the SDP Media Component Policy table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** **Note:** For each SDP media subscription profile, up to ten media component policies can be provisioned. For each media component policy, up to 20 attribute codecs can be provisioned.

Perform the following steps at the **SCSCF Tables - SDP Media Component Policy** window to add, modify, or delete the SDP Media Component Policy table attributes:

| If you want to ...                                    | then ...  |
|---|---|
| add the SDP Media Component Policy table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SDP Media Component Policy</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a SDP Media Component Policy table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SDP Media Component Policy</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                                    | then ...  |
|---|---|
| delete a SDP Media Component Policy table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

**5 Provision the parameters for the SDP Media Component Policy:**

For more information on the parameters, see the topic **SDP Media Component Policy** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

**6 Click OK.**

**Result:** The SDP Media Component Policy table attributes are provisioned successfully.

END OF STEPS

### Steps to provision a SDP media subscription profile table

Perform the following steps at the Provisioning GUI:

**1 Select IMS → IMS Components → SCSCF Tables.**

**Result:** The **SCSCF Tables** window is displayed.

**2 In the left pane, expand the SDP media subscription profile folder.**

**Result:** The SDP media subscription profile tables are listed under the folder in the left pane.

If the folder is empty, add a SDP media subscription profile table.

Perform the following steps in the **SCSCF Tables - SDP media subscription profile** window to add, rename, or delete a SDP media subscription profile table :

| If you want to ...                             | then ...   |
|--|--|
| add a SDP media subscription profile table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add SDP media subscription profile table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a SDP media subscription profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename SDP Media Subscription Profile table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a SDP media subscription profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a SDP media subscription profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>  |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the SDP media subscription profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **SCSCF Tables - SDP media subscription profile** window to add, modify, or delete the SDP media subscription profile table attributes:

| If you want to ...  | then ...   |
|---|--|
| add the SDP media subscription profile table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SDP media subscription profile</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a SDP media subscription profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SDP media subscription profile</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a SDP media subscription profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p>                               |

- 5 Provision the SDP media subscription profile parameters.

For more information on the parameters, see the topic **SDP media subscription profile** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 6 Click **OK**.

**Result:** The SDP media subscription profile table attributes are provisioned successfully.

END OF STEPS

### To provision the SDP Media MSRP table attributes

See “[To provision an SDP Media MSRP Table](#)” (p. 5-286) for the provisioning procedure information.

# To provision an S-CSCF profile

## Purpose

This procedure is used to provision an S-CSCF profile.

## Steps to provision a S-CSCF Profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → SCSCF Tables**.

**Result:** The **SCSCF Tables** window is displayed.

- 2 In the left pane, expand the **SCSCF Profile** folder.

**Result:** The SCSCF Profile tables are listed under the folder in the left pane.

If the folder is empty, add a S-CSCF Profile table.

Perform the following steps in the **SCSCF Tables** window to add, rename, or delete a S-CSCF Profile table :

| If you want to ...             | then ...  |
|--------------------------------|---|
| add a S-CSCF Profile table,    | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add SCSCF Profile table</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |
| rename a S-CSCF Profile table, | <ol style="list-style-type: none"><li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Rename SCSCF Profile table</b> window is displayed.</li><li>2. In the <b>Table Name</b> box, type a new table name.</li><li>3. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p>   |

| If you want to ...             | then ...  |
|--------------------------------|---|
| delete a S-CSCF Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a S-CSCF Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the S-CSCF Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **SCSCF Tables - SCSCF Profile** window to add, modify, or delete the S-CSCF Profile table attributes:

| If you want to ...                        | then ...  |
|---|---|
| add the S-CSCF Profile table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SCSCF Profile attributes</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a S-CSCF Profile table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SCSCF Profile attributes</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                        | then ...  |
|---|---|
| delete a S-CSCF Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters in the **Registration** tab:

| Parameter                            | Provisioning   |
|--------------------------------------|--|
| <b>Min Registration Period (sec)</b> | Type a new value.<br>Default value is 3600.  |
| <b>Emergency Registration Timer</b>  | Type a appropriate value. The timer range is 300 to 3600.<br>Default value is 900 seconds. |

6

| If you want to...                    | then...  |
|--------------------------------------|--|
| add a permanent registration set,    | <p>perform the following procedure:</p> <ol style="list-style-type: none"> <li>In the <b>Permanent Registration Set Types</b>, click <b>Add</b>.</li> <li>Select the <b>PRSET Type</b> from the drop-down list.</li> <li>Click <b>OK</b>.</li> </ol> |
| delete a permanent registration set, | <p>perform the following procedure:</p> <ol style="list-style-type: none"> <li>In the <b>Permanent Registration Set Types</b>, select the PRSET type you want to delete.</li> <li>Click <b>Delete</b>.</li> </ol>                                    |

**Note:** For more information on the parameters, see the topic **SCSCF Profile Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

- 7 Click OK.

**Result:** The S-CSCF Profile table attributes are provisioned successfully.

- 8 Provision the following parameters in the **Subscription** tab:

| Parameter  | Provisioning   |
|--|--|
| <b>Subscription Events to Record Route</b> section | Enter any five instances of <b>Event</b> with a maximum of 31 characters. The value is matched against the Event header with SUBSCRIBE or REFER. |
| <b>Min Reg Subscription Timer</b>                  | Type the minimum registration event package subscription interval.   |
| <b>Refer/Suscribe Proxy Guard Time (sec)</b>       | Type a new value or retain the default value.  |

- 9 Provision the following parameters in the **Authentication Options** tab:

| Parameter                                | Provisioning  |
|--|---|
| <b>SIP Authentication</b> section        |   |
| <b>NASS Bundled</b>                      | Select the check box to enable the NASS-bundled authentication scheme.  |
| <b>SIP-Digest</b>                        | Select the check box to authenticate the UE as the scheme.<br><br><b>Note:</b> SIP-Digest authentication scheme is mutually exclusive of Digest-MD5-A1, Digest-MD5-password and PC Digest.                          |
| <b>Authentication Parameters</b> section |   |
| <b>Authenticate Protected Register</b>   | Select check box to authenticate a protected REGISTER request.  |
| <b>Support Authentication Info</b>       | Select the check box to indicate whether the S-CSCF supports authentication information or not.<br><br><b>Note:</b> Select only when the <b>SIP-Digest</b> authentication scheme is selected in the S-CSCF Profile. |
| <b>Registration Await Auth (sec)</b>     | Retain the default value or enter a new value in the field.   |

| Parameter  | Provisioning  |
|--|---|
| <b>Registration without Auth Header</b>  | Select the appropriate value from the drop-down list. This parameter defines the action to be taken when the received REGISTER message does not have a private user identity in the Authorization header. The allowed actions are <b>Derive-PrId</b> or <b>Challenge</b> .<br><br><b>Note:</b> <b>Challenge</b> cannot be set when either <b>Early IMS Security</b> or <b>NASS Bundled</b> authentication scheme is selected. |
| <b>Authentication Options for UE-Originated Non-Register Requests</b> section.<br><br>Click <b>Add / Modify / Delete</b> in the <b>Non-Register SIP Requests</b> window to add / modify / delete an entry. |   |
| <b>SIP Request</b>   | Select the appropriate value from the drop-down box.  |
| <b>% of Request Challenged</b>   | Select the appropriate value from the drop-down box and click <b>OK</b> .   |

- 10 Provision the following parameters in the **Digit Analysis** tab.

The **Digit Analysis** tab on S-CSCF supports Digit Analysis and Normalization function.

| Parameter  | Provisioning   |
|--|--|
| <b>Invoke DA after completion of iFC Processing</b>  | Select the check box to invoke the Digit Analysis function after completion of ORIG iFC processing. If this check box is blank, then the <b>Phone Context Parameters</b> section in this tab is unavailable. |
| <b>Note:</b> The IMS Digit table and SIP Error Code table must be provisioned before provisioning the S-CSCF Profile to support Digit Analysis and Normalization function. For the provisioning task flow, see “ <a href="#">Digit Analysis and Normalization Function - Provisioning Task flow</a> ” (p. 1-55). |  |
| <b>Digit Table ID</b>  | Select the appropriate IMS Digit Table ID value from the drop-down box to specify the digit table to run for this S-CSCF.  |

**11** Provision the following parameters in the **Miscellaneous** tab.

| Parameter   | Provisioning   |
|---|--|
| <b>Transit Allowed For AS PSI Call Originations</b> | Select the check box to determine if an Application Server (AS) is enabled to include the “transit” parameter in the INVITE Route header of a SIP message.   |
| <b>BGCF Name</b>                                    | <p>Enter to define the auxiliary Breakout Gateway Control Function (BGCF) URI.</p> <p><b>Note:</b> If no value is entered in the field, the S-CSCF assigns a default BGCF URI based on the local zone domain name of the S-CSCF. If a BGCF is co-located with the S-CSCF, then call processing is normal. If the BGCF is not co-located with the S-CSCF, then the calls that lead to the BGCF will fail.</p> <p><b>P-NAPTR configuration:</b></p> <p>To use the P-NAPTR functionality, besides the P-NAPTR tables, the BGCF name must be specified using the Generic URI Label (GUL) and home domain (bgcf-stdn.example.com) instead of the GUL and local zone domain (bgcf-stdn.east.example.com). This is used to find a match in the P-NAPTR database when the S-CSCF is routing to a BGCF. The P-NAPTR database returns the BGCF's to try which includes the local zone domains in the FQDN.</p> |
| <b>ACR Charging Profile ID</b>                      | <p>Select the ID to the S-CSCF that needs to be mapped in the list.</p> <p><b>Note:</b> The default ID 0 is mapped to 3GPP version 5 ACR messages and cannot be changed. To change the version, a new ACR charging profile must be created with the expected version selection and associated with the S-CSCF.</p>   |
| <b>Emergency Session Routing Method</b>             | The values are <b>None</b> or <b>HSS</b> . Selecting <b>HSS</b> means that the S-CSCF performs a query on the <b>HSS</b> for the Emergency Services Routing Number (ESRN).   |
| <b>Support Caller Feature Preference</b>            | Use the radio buttons to activate or deactivate service preference.  |
| <b>Enum Profile ID</b>                              | Select the ID of the ENUM Profile Table that contains ENUM specific behavior used by S-CSCF determine launching an ENUM query.   |

| Parameter  | Provisioning  |
|--|---|
| <b>Generate Security Alarm for Theft of Service</b>              | <p>Use the radio buttons to activate or deactivate the generation of security alarm in case of theft of service.</p> <p>The system assumes theft of service, if the originating IMS UE includes a non-SDP or a non-ISUP message body in the SIP INVITE message, while the terminating party returns a failure response (4XX/5XX/6XX).</p> |
| <b>Enable Unregistered Origination</b>                           | Select the check box to provide services to the PBX UE as unregistered users.   |
| <b>Enforce Phone-Context When Routing Local Numbers</b>          | Select the check box to trigger the enforcement of phone-context parameters.  |
| <b>Next Hop for PBX Originations</b>                             | <p>Enter the FQDN or IP address of the default Routing Control Function.</p> <p>S-CSCF routes the call to entity addressed by this field when it finds “ims” indicator (tag) in the ENUM response. If this field is empty then S-CSCF will proceed with normal routing based on domain name in the Request URI.</p>                       |
| <b>Route requests to unregistered users based on Request-URI</b> | Select the check box to allow the S-CSCF to route terminating requests destined to unregistered subscriber based on the Request-URI, in case the host address in R-URI does not belong to one of the IMS Home Domains.  |
| <b>Pass HSS Provided CCF Address</b>                             | Select the check box to allow the S-CSCF to pass the CCF addresses provided by the HSS to other network elements in the network.  |
| <b>IBCF not Configured</b>                                       | Select the check box to indicate that IBCF is not configured in the system.   |

| Parameter   | Provisioning   |
|---|--|
| <b>Allow ODI reuse in INVITE</b>                  | <p>Select the check box to allow AS to send an INVITE request to the S-CSCF with a previously used Original Dialog Identifier (ODI) parameter in route header after the AS had already sent a final response to the original INVITE request that included the ODI definition.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>The original INVITE dialog that defined the ODI needs to be active to reuse ODI.</li> <li>Multiple INVITE requests reuse ODI either before or after final response is sent to the initial INVITE. This results in continuation of initial Filter Criteria (iFC) evaluation from the same relative position for AS.</li> <li>When the <b>Allow ODI reuse in INVITE</b> field is unchecked, the S-CSCF allows the ODI to be used for single thread of INVITE request before final response. Evaluation of the iFC occurs and the INVITE request is sent to the AS.</li> </ul> |
|   | <p><b>Support IFC Trigger for Modified Request-URI:</b> Select the appropriate value from the drop-down list. The available values are <b>None</b>, <b>Term-iFC</b> and <b>Orig-iFC</b>.</p> <p><b>Note:</b> When the AS modifies the Request-URI, then the S-CSCF processing depends on the <b>Support iFC trigger for modified Request-URI</b> parameter.</p>  |
| <b>If the parameter value is set to...</b>        | <b>then...</b>   |
| <b>None</b>                                       | the S-CSCF immediately routes the call based on the modified Request-URI.  |
| <b>Term-iFC</b>                                   | the S-CSCF continues the terminating filter criteria evaluation based on the ODI.  |
| <b>Orig-iFC</b>                                   | the S-CSCF starts the originating filter criteria evaluation based on the original served user of the terminating S-CSCF.<br><b>Note:</b> This is applicable in call forwarding scenarios.   |
| <b>Support for P-Served-User Header</b>           | To disable the support of the P-Served-User header uncheck this box.   |
| <b>Action for Redirection Responses</b>           | Select one of the available options from the drop-down box. The available options are <b>Proxy</b> , <b>Evaluate-Route</b> , and <b>Route-Direct</b> .   |
| <b>Send P-Served-User Header to BGCF</b>          | Select the check box to include the P-Served-User header in the requests sent from the S-CSCF to the BGCF.   |
| <b>Disable Diversion Case for AS Originations</b> | Select the check box to disable the use of the Diversion header present in the AS originating INVITE requests, as an alternative to the originating PSI mechanism.   |

| Parameter   | Provisioning  |
|---|---|
| <b>Support for GRUU</b>   | Select the check box, if the S-CSCF should assign GRUU to an incoming REGISTER request, with Supports/Require header containing the “+sip.instance” header parameter and an instance ID in the Contact header. This parameter is valid only for registration requests.  |
| <b>Only allow Initial SIP Requests for Subscribed ICSI and Compliant to Policy</b>                | Select the check box if the user wants the subscriber requests to meet the criteria for one of the subscribed ICSI services, like SDP/Content-Type matching an ICSI definition and the UE including an ICSI in the SIP request.   |
| <b>Only Allow Modification to SIP Dialogs that Aligns with ICSI Identified at Start of Dialog</b> | Select the check box if the user wants UPDATE/re-INVITE to include SDP/Content-Type that aligns with the original ICSI and is not allowed to change ICSI services mid-dialog.   |
| <b>Search Initial SIP Requests without ICSI for Presence of ICSI Attributes</b>                   | Select the check box if the SIP requests that don't include ICSI values are checked to see if the SDP/Content-Type in the SIP request matches the attributes for one of the subscribed ICSI services (from the HSS subscriber profile). These services are defined in the operator configured <b>ICSI Table</b> .   |
| <b>Support AliasInd</b>   | If the check box is selected, then the S-CSCF supports the “AliasInd” feature and is able to receive an AliasIdentityGroupID for each PUID in the user profile and the alias PUIDs are defined as PUIDs that have the same AliasIdentityGroupID.<br><br>If the check box is not selected, then the S-CSCF will not support the “AliasInd” feature. This means that the alias PUIDs are defined as PUIDs that are within the same implicit registration set and share the same service profile.      |
| <b>Support Loose-Route-Indication</b>   | If this check box is selected, then the S-CSCF supports receiving the Loose-Route-Indication AVP in SAA and will perform loose-route for a terminating call to the PUID if the Loose-Route-Indication is set to LOOSE_ROUTE_REQUIRED.<br><br>If this check box is not selected, then the S-CSCF does not support receiving the Loose-Route-Indication AVP in the SAA. Whether loose-route is performed or not is controlled by the existing local policy, “Routing adaptation for PBX termination”. |
| <b>Guard Timer for Unregistered PUID iFC (min)</b>  | Enter the appropriate timer value in the field. This timer determines how long the S-CSCF keeps the service profile for an unregistered PUID after the last unregistered session ends. When the timer is set to “0”, the S-CSCF removes the unregistered PUID and its service profile when the unregistered session ends.   |

| Parameter                                       | Provisioning   |
|---|--|
| <b>Guard Timer for Wildcarded PSI iFC (min)</b> | Enter the appropriate timer value in the field. This timer determines how long the S-CSCF keeps the service profile for a wildcarded PSI after an originating or terminating session from or to a wildcarded PSI ends (and the wildcarded PSI is not involved in any other session). When the timer is set to “0”, it means that the S-CSCF removes the wildcarded PSI and its service profile when the session ends and the wildcarded PSI is not in any other session. This field is applicable when the <b>Support Wildcarded PSI</b> flag is set to <b>Yes</b> . |

- 12 Provision the following parameters in the **Miscellaneous 2** tab.

| Parameter                               | Provisioning  |
|---|---|
| <b>Send Type 1 IOI Parameters to AS</b> | Select the check box if type 1 IOI parameters should be included in the P-Charging-Vector header in the third-party register messages sent to an AS. To enable this field ensure the <b>IOI Parameter</b> field in the NGSS Parameters/Timers screen is not blank.  |
| <b>Send Type 2 IOI Parameters to AS</b> | Select the check box if type 2 IOI parameters should be included in the P-Charging-Vector header in the third-party register messages sent to an AS. To enable this field ensure the <b>IOI Parameter</b> field in the NGSS Parameters/Timers screen is not blank.  |
| <b>Send Type 3 IOI Parameters to AS</b> | Select the check box if type 3 IOI parameters should be included in the P-Charging-Vector header in the third-party register messages sent to an AS. To enable this field ensure the <b>IOI Parameter</b> field in the NGSS Parameters/Timers screen is not blank.  |
| <b>SIP Error Treatment Table</b>        | To set the SIP Error Treatment Table ID referred by this profile, select a valid table ID from the list.  |
| <b>Sip Filter Set</b>                   | Select the appropriate value from the list. This list identifies the filter set that this instance uses for SIP message screening. A value of 0 (zero) specifies that SIP message screening is not configured at this instance. A non-zero value within the defined range is an index to a record in the SIP Filter Set table. If IScreen-A feature license is not provided, then the Sip Filter Set cannot be set to a non-zero value. |

| Parameter   | Provisioning   |
|---|--|
| <b>Send immediate dereg SAR for unregistered call</b> | If this check box is enabled, the S-CSCF sends an SAR to de-register a user as soon as the service profile is downloaded. The user is not de-registered locally until the <b>Guard timer for unregistered PUID iFC</b> expires.  |
| <b>Insert default PUID when invoking AS</b>           | If this check box is enabled, the S-CSCF includes a new X-ALU-DefaultPUID header that is populated with the default PUID in the same Implicit Registration Set as the calling or called party, when an AS is invoked.  |
| <b>IMS Restoration Registration Timer</b>             | If the contact header in the original register request does not include a registration time, or does not have a valid registration time, this is the default timer set for a restored registration. The default value is <b>3600</b> . The range is <b>300–600,000</b> . |

13 Click **OK**.

**Result:** The new values are updated in the profile table.

For further information related to the parameters see *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision Emergency Session Routing Method

## Purpose

This procedure is used to activate or deactivate the Emergency Session Routing Method (ESRM). This method is used to obtain an emergency routing number that routes the call to the emergency center associated with the geographic area of the call originator.

## Procedure to provision ESRM

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS > IMS Components > SCSCF Tables**.

**Result:** The **SCSCF Tables** window is displayed.

- 2 In the left pane, expand the **SCSCF Profile** folder.

**Result:** The **SCSCF Profile** tables are listed under the folder in the left pane.

If the folder is empty, add a **SCSCF Profile** table.

Perform the following steps in the **SCSCF Profile Attributes** window to add, rename, or delete a **SCSCF Profile** table :

- 3 Provision the following parameters in the **Miscellaneous** tab:

| Parameter                               | Provisioning  |
|---|---|
| <b>Emergency Session Routing Method</b> | Use this field to activate or deactivate ESRM. The values are <b>None</b> or <b>HSS</b> . Select <b>HSS</b> to activate and <b>None</b> to deactivate the ESRM. |

For further information on the parameters, see the topic **ECSCF Profile Table** in the *Alcatel-Lucent Control Platform 1800/1000/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

- 4 Click **OK**.

**Result:** The **Emergency Session Routing Method** is provisioned successfully.

END OF STEPS

# To provision support for wildcard PUID

## Purpose

This procedure is used to support wildcard PUID.

## Before you begin

This procedure is performed at the Provisioning GUI.

## Procedure to provision support for wildcard PUID

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS > IMS Components > SCSCF Tables**.
- 2 In the left pane, expand the **SCSCF Profile** folder.
- 3 Click the required profile and select **Open** from the **Tables** menu.
- 4 Select **Modify Table Attributes** from the **Attributes** menu.  
**Result:** The **SCSCF Profile Attributes** window is displayed.
- 5 Provision the following parameters in the **Miscellaneous** tab.

| Parameter                                     | Provisioning   |
|---|--|
| <b>Routing adaptation for PBX termination</b> | Select the required option from the list.<br>This parameter defines if special handling is needed for routing a termination request to a PBX using Wildcard PUID. If set to <b>None</b> , then no special processing is performed by the S-CSCF for session request to a PUID that matches a wildcard PUID. If set to <b>Loose-Route</b> , the S-CSCF inserts an additional Route header that is populated with the registered contact address. It does not change the received R-URI. |

| Parameter                            | Provisioning   |
|--------------------------------------|--|
| R-URI adaptation for PBX termination | Select the required option from the list.<br><br>This parameter defines if Request- URI adaptation is needed for PBX termination using wildcard PUID. This parameter is only applicable when the <b>Routing adaptation for PBX termination</b> is enabled. If set to <b>SIP URI</b> , the S-CSCF converts the R-URI from tel URI to SIP URI, using the host portion from the default pbxPUID. If set to <b>None</b> , then no adaptation is performed. |

For further information on the parameters see the topic **SCSCF Profile Table** in the *Alcatel-Lucent Control Platform 1800/1000/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

- 
- 6 Click OK.

**Result:** The support for wildcard PUID is provisioned successfully.

END OF STEPS

---

# To activate PacketCable authentication in an S-CSCF profile

## Purpose

This procedure is used to activate PacketCable authentication in an S-CSCF profile.

**Note:** The PacketCable authentication is mutually exclusive with NASS-Bundled and EIS authentication. Therefore, when an S-CSCF profile is provisioned for the PacketCable authentication, it is not allowed to use the same S-CSCF profile for EIS or NASS-Bundled authentication and vice-versa.

## Before you begin

Ensure the S-CSCF is available in the network.

### Frequency

This procedure must be performed for each S-CSCF.

### System requirements

Provisioning GUI connection.

## Procedure to activate PacketCable authentication in an S-CSCF profile

Perform the following steps at the Provisioning GUI:

1 Select **IMS > IMS Components > SCSCF Tables**.

2 In the left pane, expand the **SCSCF Profile** table folder.

3 Click the required entry and select **Open** from the **Tables** menu.

**Result:** The **SCSCF Profile Attributes** window is displayed.

4 Select **Modify Table Attributes** from the **Attributes** menu.

5 In the **Authentication Options** tab, select the required **Digest** check box.

**Note:** The associated HSS must advertise that it supports the Supported-Vendor-Id AVP = PacketCable for Digest authentication to work. Digest authentication requires the SIP-Digest- Authenticate AVP from the HSS. The PacketCable Vendor ID is 4491.

6 Click **OK**.

**Result:** The new values are updated.

For further information on the parameters see *Alcatel-Lucent Control Platform 1800/1000/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision a S-CSCF PSI URI table

## Purpose

This procedure is used to provision a S-CSCF PSI URI table.

## Steps to provision a S-CSCF PSI URI table

Perform the following steps at the Provisioning GUI:

1 Select **IMS > IMS Components > SCSCF Tables**.

2 In the left pane, expand the **S-CSCF PSI URI** folder.

**Result:** The S-CSCF PSI URI tables are listed under the folder in the left pane.

If the folder is empty, add a S-CSCF PSI URI table.

Perform the following steps in the **S-CSCF Tables - S-CSCF PSI URI** window to add, rename, or delete a S-CSCF PSI URI table :

| If you want to ...             | then ...   |
|--------------------------------|--|
| add a S-CSCF PSI URI table,    | <ol style="list-style-type: none"><li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add S-CSCF PSI URI table</b> window is displayed.</li><li>From the <b>Table Number</b> list, select the table number.</li><li>In the <b>Table Name</b> box, type a descriptive table name.</li><li>Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |
| rename a S-CSCF PSI URI table, | <ol style="list-style-type: none"><li>Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Rename S-CSCF PSI URI table</b> window is displayed.</li><li>In the <b>Table Name</b> box, type a new table name.</li><li>Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p>  |

| If you want to ...             | then ...  |
|--------------------------------|---|
| delete a S-CSCF PSI URI table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a S-CSCF PSI URI table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Click on the **Attributes** menu and select **Add Table Attributes**.

**Result:** The **Add S-Cscf PSI URI** window is displayed.

- 4 Select the following values in the **Add S-CSCF PSI URI** window:

| Parameter         | Value  |
|-------------------|--|
| <b>PSI URI ID</b> | Select the URI ID value from 01 to 50 from the drop down.<br>Up to 50 PSI URI IDs can be provisioned.          |
| <b>PSI URI</b>    | Enter the URI with a maximum of 256 characters. The first four characters must be <b>sip:</b> or <b>SIP:</b> . |

- 5 Click **OK**.

**Result:** A new S-CSCF PSI URI entry is added to the **SCSCF PSI URI** table.

For further information on the parameters see the topic **SCSCF PSI URI** in the *Alcatel-Lucent Control Platform 1800/1000/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision a Home Network Identifier profile table

## Purpose

This procedure is used to add, modify, or delete the Home Network Identifier profile table. This table is used by the S-CSCF to determine the connectivity status of P-CSCF in the home network.

## Steps to provision a Home Network Identifier profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS > IMS General Tables**.

**Result:** The **IMS General Tables** window is displayed.

- 2 In the left pane, expand the **Home Network Identifier** folder. If the folder is empty, add a Home Network Identifier table.

- 3 Perform the following steps in the **Home Network Identifier** window to add, rename, or delete a Home Network Identifier table :

| If you want to ...                           | then ...  |
|--|---|
| add a Home Network Identifier table,         | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Home Network Identifier</b> window is displayed.</li><li>2. From the <b>Network Identifier Index</b> list, select the number.</li><li>3. In the <b>Network Identifier</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.<br/>The user can add only one table.<br/><i>End of steps</i></li></ol> |
| rename a Home Network Identifier table name, | <ol style="list-style-type: none"><li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Home Network Identifier</b> window is displayed.</li><li>2. In the <b>Table Name</b> box, type a new table name.</li><li>3. Click <b>OK</b>.<br/><i>End of steps</i></li></ol>   |

| If you want to ...                      | then ...  |
|---|---|
| delete a Home Network Identifier table, | <ol style="list-style-type: none"> <li>1. Select the table, and then <b>Tables</b> → <b>Delete table</b> from the menu.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Home Network Identifier table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 4 Click **Attributes** menu and select **Add Table Attributes**.

**Result:** The **Home Network Identifier** window is displayed.

- 5 Select the **Network Identifier Index** from the drop-down box.

**Note:** The Network Identifier Index is unique and up to ten Network Identifier records can be provisioned. This field must not be null.

- 6 Enter the network field in the **Network Identifier** text box.

The maximum number of characters in this field is 128.

- 7 Click **OK**.

**Result:** A new Home Network Identifier entry is added to the **Home Network Identifier** table.

For further information on the parameters see **Home Network Identifier Table** in the *Alcatel-Lucent Control Platform 1800/1000/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To activate enhanced third party registration

## Purpose

This procedure is used to activate enhanced third party registration.

## Before you begin

**System requirements:** Ensure S-CSCF is available in the network.

## Procedure to activate enhanced third party registration in the S-CSCF profile

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS > IMS Components > SCSCF Tables**.
- 2 In the left pane, expand the **SCSCF Profile** folder.
- 3 Click the required table entry and select **Open** from the **Tables** menu to open the table.
- 4 Click the required table entry and select **Modify Table Attributes** from the **Attributes** menu.
- 5 In the **Registration** tab, select the **Send Enhanced 3rd Party REGISTER** check box.
- 6 Click **OK**.

**Result:** The enhanced third party registration is activated in the S-CSCF profile.

For further information on the parameters see *Alcatel-Lucent Control Platform 1800/1000/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision the S-CSCF profile to support IP-PBX calls

## Purpose

This procedure is used to provision the S-CSCF profile to support IP-PBX calls.

## Before you begin

- Provisioning data to complete the procedure.
- Ensure the profile is not used by the SIPia port before deleting an S-CSCF profile table.

## Steps to provision an S-CSCF profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS > IMS Components > SCSCF Tables**.
- 2 In the left pane, expand the **SCSCF Profile** folder. If the folder is empty, add a **SCSCF Profile** table.
- 3 Perform the following steps in the **SCSCF Tables** window to add, rename, or delete a SCSCF Profile table:

| If you want to ...              | then ...  |
|---------------------------------|---|
| add an S-CSCF Profile table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add SCSCF Profile table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <i>End of steps</i> |
| rename an S-CSCF Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Rename SCSCF Profile table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <i>End of steps</i>  |

| If you want to ...              | then ...   |
|---------------------------------|--|
| delete an S-CSCF Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>OK</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a S-CSCF Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 4 Select **Attributes** menu and **Modify Table Attributes**. To support IP-PBX calls, provision the following parameters in the **S-CSCF Profile Attributes** screen, **Subscription** tab:

| Parameter                                    | Provisioning  |
|--|---|
| <b>Subscription Events to Record Route</b>   | Enter five instances of <b>Event</b> with a maximum of 31 characters. The value is matched against the Event header with SUBSCRIBE and implicitly with REFER. |
| <b>Min Reg Subscription Timer</b>            | Select the default value or enter a new value.  |
| <b>Refer/Suscribe Proxy Guard Time (sec)</b> | Select the default value or enter a new value.  |

- 5 Provision the following parameters in the **Miscellaneous** tab.

| Parameter   | Provisioning   |
|---|--|
| <b>Transit Allowed For AS PSI Call Originations</b> | Select to determine if an Application Server (AS) is enabled to include the “transit” parameter in the INVITE Route header of a SIP message.   |
| <b>BGCF Name</b>                                    | <p>Enter the name of auxiliary Breakout Gateway Control Function (BGCF) URI.</p> <p><b>P-NAPTR configuration:</b></p> <p>To use the P-NAPTR functionality, besides the P-NAPTR tables, the BGCF name must be specified using the Generic URI Label (GUL) and home domain (bgcf-stdn.example.com) instead of the GUL and local zone domain (bgcf-stdn.east.example.com). These values are used to find a match in the P-NAPTR database when the S-CSCF is routing to a BGCF. The P-NAPTR database returns the BGCF which includes the local zone domains in the FQDN.</p> |

| Parameter  | Provisioning   |
|--|--|
| <b>Emergency Session Routing Method</b>                              | Select the available values <b>None</b> or <b>HSS</b> from the drop-down. By selecting <b>HSS</b> , S-CSCF performs a query on the HSS for the Emergency Services Routing Number (ESRN).   |
| <b>Enum Profile ID</b>   | Select the ID of the ENUM profile table that contains ENUM specific behaviors that the S-CSCF requires to launch for an ENUM query in the list.  |
| <b>Generate Security Alarm for Theft of Service</b>                  | Use the radio buttons to activate or deactivate the generation of security alarm in case of theft of service.<br><br>The system assumes theft of service, if the originating IMS UE includes a non-SDP or a non-ISUP message body in the SIP INVITE message, while the terminating party returns a failure response (4XX/5XX/6XX).   |
| <b>Enable Unregistered Origination</b>                               | Select the check box to provide services to the PBX UE as unregistered users.  |
| <b>Enforce Phone-Context When Routing Local Numbers</b>              | Select the check box to trigger the enforcement of phone-context parameter.  |
| <b>Next Hop for PBX originations</b>                                 | Enter the FQDN or IP address of the default Routing Control Function in this field. S-CSCF routes the call to entity addressed by this field when it finds “ims” indicator (tag) in the ENUM response. If this field is empty then S-CSCF proceeds with the normal routing based on domain name in the Request URI.  |
| <b>Route requests to unregistered users based on the Request-URI</b> | Select the check box to allow the S-CSCF to route terminating requests destined to unregistered subscribers based on the Request-URI if the host address in the R-URI does not belong to one of the IMS Home Domains.  |
| <b>Routing adaptation for PBX termination</b>                        | Select the available options from the drop-down box.<br><br><b>Note:</b> This parameter defines if special handling is needed for routing a termination request to a PBX using wildcard PUID. If set to <b>None</b> , then no special handling is performed by the S-CSCF for session request to a PUID that matches a wildcard PUID. If set to <b>Loose-Route</b> , the S-CSCF inserts an additional Route header that is populated with registered contact address. It does not change the received R-URI. |

| Parameter                            | Provisioning   |
|--------------------------------------|--|
| R-URI adaptation for PBX termination | Select the available options from the drop-down box.<br><b>Note:</b> This parameter defines if Request- URI adaptation is needed for PBX termination using wildcard PUID. This parameter is only applicable when the <b>Routing adaptation for PBX termination</b> is enabled. If set to <b>SIP URI</b> , the S-CSCF converts the R-URI from tel URI to SIP URI, using the host portion from the default pbxPUID. If set to <b>None</b> , then no adaptation is performed. |

**Note:** For further information on the parameters see *Alcatel-Lucent Control Platform 1800/1000/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

- 6 Click **OK**.

**Result:** The new values are updated.

END OF STEPS

---

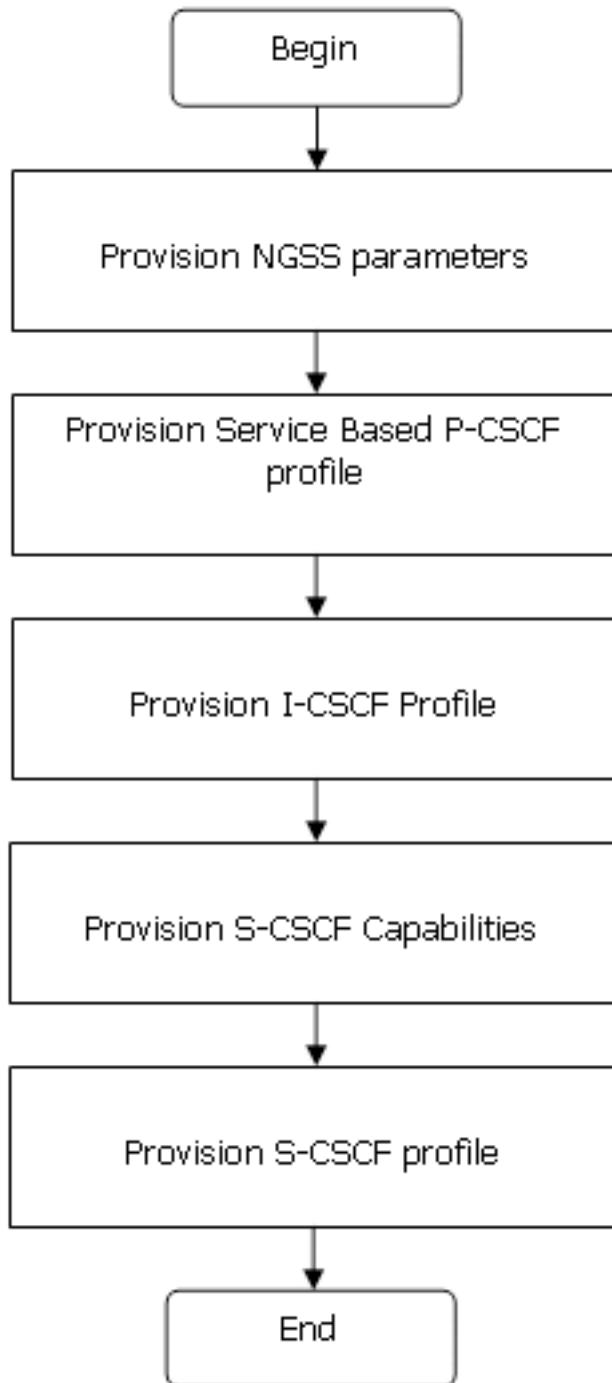
## Provisioning Task flow - To provision S-CSCF pool

### Purpose

This provisioning task flow provides the steps to provision S-CSCF pool.

## Provisioning task flow diagram

The following figure illustrates the provisioning task flow for provisioning the S-CSCF pool.



## Steps to provision the S-CSCF pool

Perform the following steps to provision the S-CSCF pool:

---

### 1 Provision the NGSS Parameters.

Provision the following parameters:

- Enable **IMS restoration Procedures**
- Enable **S-CSCF pool mode**

See “[To provision NGSS Server parameters](#)” (p. 10-9).

---

### 2 Provision a Service Based P-CSCF profile.

Provision the following parameters:

- Enable **Heartbeat S-CSCF**
- Set the **Tss Timer (secs)**
- Set the **Tsf Timer (secs)**

See “[To provision Service-Based PCSCF Profile](#)” (p. 4-69).

---

### 3 Provision an I-CSCF Profile.

Provision the following parameters:

- Set **Max S-CSCF Retry** to the number of S-CSCF in a pool
- Set **Register Without Authorization header** to set IMPI to Zero
- Enable **S-CSCF Selection with User Number**

See “[To provision ICSCF Profile](#)” (p. 4-45).

---

### 4 Provision S-CSCF Capabilities.

Add S-CSCF in a pool with the same capabilities

See “[To provision the S-Cscf Capability List](#)” (p. 4-53).

**Note:**

- This configuration is useful only when HSS configured the UE with same capability.
  - If S-CSCF FQDN is configured and the S-CSCFs within a pool are in different system, DNS is needed.
- 

### 5 Provision an S-CSCF profile

---

Select **Enable Unregistered Origination**.

See “[To provision an S-CSCF profile](#)” (p. 4-15).

# I-CSCF provisioning

## Overview

### Purpose

This section provides the procedures that are used to provision the Interrogating CSCF (I-CSCF).

### Contents

|   |      |
|---|------|
| To provision ICSCF Profile              | 4-45 |
| To provision the S-Cscf Capability List | 4-53 |
| To create a PSI sub-domain list         | 4-57 |

# To provision ICSCF Profile

## Purpose

This procedure is used to provision an ICSCF Profile.

## When you *add* an ICSCF Profile table

When you *add* a new ICSCF Profile table, the table is empty. You must add an ICSCF Profile.

## Before you *delete* an ICSCF Profile table

Before you *delete* an ICSCF Profile table, ensure that the profile is NOT used by an SIPia port.

## Before you begin

Observe the following:

### Frequency

This procedure must be performed whenever an ICSCF Profile table must be provisioned.

### Required information

Provisioning data to complete the procedure.

This procedure is performed at the Provisioning GUI.

## Steps to provision a ICSCF Profile table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS → IMS Components → ICSCF Tables**.

**Result:** The **ICSCF Tables** window is displayed.

---

- 2 In the left pane, expand the **ICSCF Profile** folder.

**Result:** The ICSCF Profile tables are listed under the folder in the left pane.

If the folder is empty, add a ICSCF Profile table.

Perform the following steps in the **ICSCF Tables** window to add, rename, or delete a ICSCF Profile table :

| If you want to ...            | then ...   |
|-------------------------------|--|
| add a ICSCF Profile table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>ICSCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a ICSCF Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>ICSCF Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |
| delete a ICSCF Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a ICSCF Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>   |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the ICSCF Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **ICSCF Tables** window to add, modify, or delete the ICSCF Profile table attributes:

| If you want to ...                       | then ...  |
|--|---|
| add the ICSCF Profile table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>ICSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <i>End of steps</i>  |
| modify a ICSCF Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>ICSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <i>End of steps</i> |
| delete a ICSCF Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <i>End of steps</i>             |

- 5 Provision the following parameters:

| Parameter               | Provisioning   |
|-------------------------|--|
| <b>Max S-CSCF Retry</b> | Enter a value in <b>Max S-CSCF Retry</b> to define the number of times an I-CSCF retries to select an S-CSCF for initial registration. |

| Parameter                          | Provisioning  |
|------------------------------------|---|
| <b>SCSCF URI</b>                   | <p>If required, enter a <b>SCSCF URI</b> to define the auxiliary Serving Call Session Control Function (S-CSCF) URI.</p> <p><b>P-NAPTR configuration:</b> To use the P-NAPTR functionality, besides the P-NAPTR tables, specify the SCSF name. Use the Generic URI Label (GUL) and home domain (scsf-stdn.example.com) instead of the GUL and local zone domain (scsf-stdn.east.example.com). This is used to find a match in the P-NAPTR database. The P-NAPTR database returns the S-CSCFs to try which S-CSCF includes the local zone domains in the FQDN.</p> |
| <b>BGCF URI</b>                    | <p>If required, enter a <b>BGCF URI</b> to define the auxiliary Breakout Gateway Control Function (BGCF) URI.</p> <p><b>Note:</b> If no value is entered in the <b>BGCF URI</b> field, the I-CSCF assigns a default BGCF URI based on the local zone domain name of the I-CSCF. If a BGCF is co-located with the I-CSCF, then call processing is normal. If the BGCF is not co-located with the I-CSCF, then the calls that lead to the BGCF will fail.</p>   |
| <b>PSI Subdomain List ID</b>       | If required, select a previously refined <b>PSI Subdomain List ID</b> from the menu.  |
| <b>Originating Host List Index</b> | Select the Originating Host List index from the <b>Originating Host List Index</b> list.  |
| <b>ENUM Profile Index</b>          | Select the ENUM Profile index from the <b>ENUM Profile Index</b> list.  |
| <b>Address Resolution Method</b>   | <p>Select one of the following from the <b>Address Resolution Method</b> list:</p> <ul style="list-style-type: none"> <li>• Cx only</li> <li>• ENUM only</li> <li>• ENUM before Cx</li> <li>• Cx before ENUM</li> </ul>   |

| Parameter   | Provisioning   |
|---|--|
| <b>Change SIP URI to TEL URI</b>                          | <p>For Multiple Home Domains configuration, check <b>Change SIP URI to TEL URI</b>.</p> <p><b>Note:</b> The HSS must be provisioned with TEL URI for every SUBSCRIBER.</p>   |
| <b>S-CSCF Selection With User Number</b>                  | <p>Select the check box to indicate that the CT S-CSCF Selection is enabled</p>  |
| <b>Enforce Phone-Context When Routing Local Numbers</b>   | <p>If required, select <b>Enforce Phone-Context When Routing Local Numbers</b> to trigger the enforcement of phone-context parameter.</p>  |
| <b>Additional Cx query</b>                                | <p>If required, select <b>Yes</b> in the <b>Additional Cx query</b> field.</p> <p><b>Note:</b> This field will be enabled only when the Address Resolution Method is set to 'Cx before ENUM'.</p>  |
| <b>Try Cx Query if ENUM result is NXDOMAIN or timeout</b> | <p>If required, select <b>Yes</b> in the <b>Try Cx Query if ENUM result is NXDOMAIN or timeout</b> field.</p> <p><b>Note:</b> This field is only applicable if ENUM is performed before Cx, that is, the "Address Resolution Method" is set to "ENUM before Cx".</p> |
| <b>Post Route Selection</b>                               | <p>Select the post route selection in the <b>Post Route Selection</b> field.</p>   |
| <b>Route Based on CgPN</b>                                | <p>If required, select <b>Yes</b> in the <b>Route Based on CgPN</b> field.</p> <p><b>Note:</b> This field is enabled only when the Address Resolution Method is set 'ENUM before Cx' or 'Cx before ENUM'.</p>  |

| Parameter                               | Provisioning   |
|---|--|
| <b>ACR Charging Profile ID</b>          | <p>Select the ACR Charging Profile ID to which the I-CSCF needs to be mapped in the <b>ACR Charging Profile ID</b> list.</p> <p><b>Note:</b> ACR Charging Profile with ID 0 is regarded as a default profile. The default profile is mapped to 3GPP version 5 ACR messages. The content of default profile is not changeable through the FS GUI. If the I-CSCF is correlated to default profile and you need to change the version, you can add a new ACR charging profile with the expected version selection and associate the I-CSCF to the new ACR charging profile.</p> |
| <b>Apply NTM prior to ENUM</b>          | <p>Select the <b>Apply NTM prior to ENUM</b> check box to apply NTM control prior to ENUM.</p>   |
| <b>Action for Redirection Responses</b> | <p>Select one of the following options from the <b>Action for Redirection Responses</b> drop-down box.</p> <ul style="list-style-type: none"> <li>• Proxy</li> <li>• Evaluate-Route</li> <li>• Route-Direct</li> </ul>   |
| <b>CANM URI</b>                         | <p>Select the appropriate value from the <b>CANM URI</b> drop-down list.</p> <p>This parameter defines the Common Announcement Module URI that is provisioned for a component that needs to send requests to the CANM to play an announcement on behalf of the component.</p>  |
| <b>Support P-Served-User Header</b>     | <p>Select <b>Support P-Served-User Header</b>.</p> <p>This option controls whether I-CSCF supports P-Served-User header, specifically, whether I-CSCF can do Cx or ENUM query based on PUID from P-Served- User header, and whether I-CSCF pass this header to S-CSCF.</p>   |

| Parameter   | Provisioning  |
|---|---|
| <b>Response code for De-Registration to Remote S-CSCF</b> | <p>Select the appropriate value from the <b>Response code for De-Registration to Remote S-CSCF</b>.</p> <p>There are two values namely <b>200 OK</b> and <b>403 Forbidden</b>.</p> <p>This option specifies the response code the I-CSCF returns for de-registration requests destined to a remote S-CSCF. The default value is to return 200 OK as the I-CSCF does, before this option was introduced. This field is applicable only if the NGSS field <b>UE Reregistration for Geo-Redundancy</b> is enabled. If the <b>UE Re-registration for Geo-Redundancy</b> field is disabled, this field should be grayed out.</p> |
| <b>SIP Error Treatment Table</b>                          | <p>To set the SIP Error Treatment Table ID referred by this profile, select a valid table ID from the <b>SIP Error Treatment Table</b> drop down list.</p>  |
| <b>SIP Filter Set</b>                                     | <p>Select the appropriate value from the <b>SIP Filter Set</b> list.</p> <p>This list identifies the Filter Set that this instance uses for SIP message screening. A value of 0 (zero) specifies that SIP message screening is not configured at this instance. A non-zero value within the defined range is an index to a record in the SIP Filter Set table.</p> <p><b>Note:</b> If IScreen-A feature license is not provided, the Sip Filter Set cannot be set to a non-zero value.</p>  |
| <b>3GPP S-CSCF Reselection for REGISTER message</b>       | <p>The I-CSCF queries the HSS to re-select an S-CSCF whenever it fails to reach SCSCF. If this flag is set, the I-CSCF verifies the rules defined by 3GPP 24.229 before performing the reselection. This flag is applicable to UAR during registration.</p>   |

For more information on the parameters, see the topic **Icscf Profile Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The ICSCF Profile table attributes are provisioned successfully.

END OF STEPS

---

# To provision the S-Cscf Capability List

## Purpose

This procedure is used to provision the S-Cscf Capability List.

This optional service is used by the I-CSCF to determine the best suited S-CSCF (or retries the next best SCSCF in case of routing failure). The selection is only performed when S-CSCF capabilities are returned by the HSS.

The S-Cscf Capability List is used to map a set of S-CSCF capabilities to fully qualified domain name (FQDN) of an SCSCF supporting those capabilities.

The S-Cscf Capability List has a maximum of 25 records and each record can map an FQDN of SCSCF to up to 10 capabilities. The entries in the capability list must be unique and they are sorted in the GUI in an ascending order.

## Steps to provision an S-Cscf Capability List table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → ICSCF Tables**.

**Result:** The **ICSCF Tables** window is displayed.

- 2 In the left pane, expand the **S-Cscf Capability List** folder.

**Result:** The S-Cscf Capability List tables are listed under the folder in the left pane.

If the folder is empty, add an S-Cscf Capability List table.

Perform the following steps in the **ICSCF Tables** window to add, rename, or delete an S-Cscf Capability List table :

| If you want to ...                   | then ...   |
|--------------------------------------|--|
| add an S-Cscf Capability List table, | <ol style="list-style-type: none"><li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add S-Cscf Capability List table</b> window is displayed.</li><li>From the <b>Table Number</b> list, select the table number.</li><li>In the <b>Table Name</b> box, type a descriptive table name.</li><li>Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |

| If you want to ...                      | then ...  |
|---|---|
| rename an S-Cscf Capability List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Add S-Cscf Capability List table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete an S-Cscf Capability List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an S-Cscf Capability List table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>              |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the S-Cscf Capability List table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **ICSCF Tables - S-Cscf Capability List** window to add, modify, or delete the S-Cscf Capability List table attributes:

| If you want to ...                               | then ...   |
|--|--|
| add the S-Cscf Capability List table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Add S-CSCF Capabilities</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                                 | then ...   |
|--|--|
| modify an S-Cscf Capability List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The Add S-CSCF Capabilities window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete an S-Cscf Capability List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                    |

**5** Provision the following parameters:

| Parameter                    | Provisioning   |
|------------------------------|--|
| <b>FQDN of S-CSCF</b>        | Type an FQDN of the S-CSCF.<br>The FQDN is the full name of a system, consisting of its local host name and its domain name, including a top-level domain. For example, "lucentcp" is a host name and "lucentcp1.operator.com" is an FQDN. Using a DNS it should be possible to resolve an FQDN towards one ore more IP addresses. |
| <b>Capability List</b> group | To add an S-CSCF capability, perform the following steps: <ul style="list-style-type: none"> <li>Click <b>Add</b>. The <b>Add S-Cscf Capability</b> window is displayed.</li> <li>Type the S-Cscf capability number and click <b>OK</b>.</li> </ul> You can add up to ten capabilities for the S-CSCF.                             |

For more information on the parameters, see the topic **S-Cscf Capabilities List** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The S-CSCF Capability List table attributes are provisioned successfully.

END OF STEPS

---

# To create a PSI sub-domain list

## Purpose

This procedure is used to add, modify, or delete a PSI sub-domain list

## Usage

Sub domains may be defined for Public Service Identities (PSIs) that allow specific PSIs within subdomains to be assigned for specific applications. Subdomains can be defined within the DNS infrastructure.

Subdomain based PSIs are globally routable and can be made available to users within and outside the operator domain.

In particular, the PSI is resolved by the global DNS to an I-CSCF address in the domain where the Application Server (AS) hosting the PSI is located.

The I-CSCF:

1. recognizes the sub domain (and thus does not query the HSS).
2. resolves the same PSI to the address of the actual destination AS hosting the PSI (using an internal DNS mechanism)
3. forwards the requests directly to the AS.

Up to 50 sub-domains can be created in one PSI sub-domain List. Up to 5 PSI sub-domain List tables may be supported. ICSCF profiles can choose one PSI subdomain ID. Each PSI subdomain has one PSI subdomain ID, while each PSI subdomain list has one PSI subdomain List ID (a.k.a PSI subdomain List table ID on the left tree view).

## When you *create* a PSI sub-domain list

After you *create* a PSI sub-domain list you must still associate the PSI sub-domain list with the I-CSCF profile.

## Before you *delete* a PSI sub-domain list

Before you delete a PSI sub-domain list, you must make sure that it is NOT referenced by an I-CSCF profile

## Before you begin

Observe the following:

### Frequency

This procedure must be carried out whenever an PSI sub-domain list must be created.

### Required information

Provisioning data to complete the procedure.

This procedure is performed at the FS GUI.

### Configuration requirements

Up to 5 PSI Sub Domain Lists may be configured and each can contain up to 50 sub domains.

**Important!** *DO NOT* to include home domain on the list of PSI sub domains. If it were included, all the calls terminated to this network will attempt to match sub domain first, leading to delay in processing the call.

The following provision rules must be followed when adding an entry into a PSI subdomain list:

- Each entry must have valid domain name
- Each domain name shall not be the same as provisioned home domain(s), otherwise, all requests coming to I-CSCF will trigger DNS query.
- When provisioning a **PSI subdomain list** for ICSCF, the URL must be added to the **served host** table of the ICSCF or the ICSCF may reject PSI requests with that domain name.

For example, if a PSI domain name is "psias.lucent.com", users need to add either "\*.lucent.com" or "psias.lucent.com" into the **served hosts** table of ICSCF.

**Important!** There is no domain syntax checking when creating a new domain name, make sure the entered sub-domain name is valid!

### PSI sub-domain list procedure

Perform the following steps at the Provisioning GUI:

1 Select **IMS** → **IMS Tables**→**IMS**→**General**→**PSI Subdomain List**.

2 In the left pane, expand the **PSI Subdomain List** folder.

| 3 | If you want to ...     | then ...  |
|---|------------------------|---|
|   | Add PSI Subdomain List | <ol style="list-style-type: none"> <li>1. Select <b>PSI Subdomain List</b> → <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add PSI Subdomain List table</b> window is displayed.</li> <li>2. Select <b>Table Number</b> and type the name of <b>PSI Subdomain List</b> into the <b>Table Name</b> field to identify the list.</li> <li>3. Click <b>OK</b>.<br/><i>End of steps</i></li> </ol> |

| If you want to ...         | then ...   |
|----------------------------|--|
| Delete PSI Subdomain List, | <p>Select the PSI Subdomain List that you want to delete, then select <b>Tables-&gt;Delete Table</b> from the menu.</p> <p>Click <b>OK</b>.</p> <p>End of procedure.</p> <p><b>Important!</b></p> <p>Please make sure no <b>PSI Subdomain ID</b> and <b>PSI Subdomain</b> are associated with the PSI Subdomain List. In case there are, then:</p> <ul style="list-style-type: none"> <li>• select the entries, right-click, select <b>Delete Table Attributes</b></li> <li>• select <b>File → Save</b> from the menu</li> </ul> |

- 
- 4 To add table attributes, select subdomain entry list, and **Attributes → Add Table Attributes** from the menu. Choose a **PSI Subdomain List ID** from the drop down and type the URI of the desired sub domain in the **PSI Subdomain** field.
- 
- 5 Click **OK**.
- Result:** A new **PSI Subdomain List** is added.
- 
- 6 At the Provisioning GUI main menu, select **IMS → IMS Tables→IMS→ICSCF→I-Cscf Profile**.
- 
- 7 Right-click the desired entry. Select **Open** from the pull-down menu to open the table. Double-click the entry in the right window.
- Result:** The **ICSCF Profile Attributes** window opens.
- 
- 8 From the drop down menu in the **PSI Subdomain List ID** field, select the desired list.
- 
- 9 Click **OK**.
- 
- 10 At the Provisioning GUI main menu, select **IMS → IMS Tables→IMS→ICSCF→ICSCF Profile**.

- 
- 11 Right-click the desired entry. Select **Open** from the pull-down menu to open the table.  
Double-click the entry in the right window.

**Result:** The **ICSCF Profile Attributes** window opens.

---

- 12 From the drop down menu in the **PSI Subdomain List ID** field, select the desired list.
- 

- 13 Click **OK**.

E N D O F S T E P S

---

# P-CSCF provisioning

## Overview

### Purpose

This section provides the procedures that are used to provision the Proxy CSCF (P-CSCF).

### Contents

|  |       |
|--|-------|
| To provision a Session Description Protocol Profile          | 4-62  |
| To provision Service-Based PCSCF Profile                     | 4-69  |
| To provision SIP Stack Timer Profile                         | 4-74  |
| To provision PCSCF profile                                   | 4-77  |
| To provision PBX Table Entry                                 | 4-96  |
| To activate the SIP header reduction                         | 4-101 |
| To activate Service Route header                             | 4-102 |
| To activate PacketCable authentication in the P-CSCF profile | 4-104 |
| To provision SIP compression                                 | 4-106 |
| To provision IMS Signaling security                          | 4-108 |
| To provision the Service Based Local Policy Profile          | 4-111 |
| To provision e2 interface support                            | 4-116 |
| Support to provide P-CSCF IP address to UE                   | 4-120 |
| To provision the TLS Profile table                           | 4-121 |
| To provision the SIP Error Treatment Table attributes        | 4-123 |
| Provisioning Task flow - To provision P-CSCF pool            | 4-126 |

# To provision a Session Description Protocol Profile

## Purpose

This procedure is used to add, modify or delete a Session Description Protocol (SDP) profile.

For Quality of Service (QoS) purposes, an SDP profile is used by the P-CSCF and the S-CSCF to examine the SDP offer/answer against the network local policies.

The P-CSCF and S-CSCF validate the SDP offer and SDP answer against Local/Network policy and take necessary actions if SDP validation fails. These actions include releasing the call or just rejecting new SDP offer and falling back on previously validated SDP.

An SDP profile includes:

- Validation of the SDP offer/answer initiated by a UE
- Validation of the SDP offer/answer initiated by the network
- Acceptable list of codec and bandwidth for default audio and video type.

## Steps to provision a Session Description Protocol Profile table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS → IMS General Tables**.

**Result:** The **IMS General Tables** window is displayed.

---

- 2 In the left pane, expand the **Session Description Protocol Profile** folder.

**Result:** The Session Description Protocol Profile tables are listed under the folder in the left pane.

If the folder is empty, add a Session Description Protocol Profile table.

Perform the following steps in the **IMS General Tables** window to add, rename, or delete a Session Description Protocol Profile table :

| If you want to ...                                   | then ...   |
|--|--|
| add a Session Description Protocol Profile table,    | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>IMS General Tables</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a Session Description Protocol Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>IMS General Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a Session Description Protocol Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Session Description Protocol Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>                                  |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the Session Description Protocol Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **IMS General Tables** window to add, modify, or delete the Session Description Protocol Profile table attributes:

| If you want to ...  | then ...   |
|---|--|
| add the Session Description Protocol Profile table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>IMS General Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a Session Description Protocol Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>IMS General Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a Session Description Protocol Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p>                   |

- 5 Provision the following parameters:

| Parameter                              | Provisioning   |
|--|--|
| <b>Session Description Protocol Id</b> | In the <b>Session Description Protocol Id</b> list, select the SDP profile ID.   |
| <b>Profile Description</b>             | In the <b>Profile Description</b> field, enter a description of the SDP profile. |

| Parameter                       | Provisioning  |
|---------------------------------|---|
| Offer/Answer Validation Options | <p>Under <b>Offer/Answer Validation Options</b>, check the SDP offer/answer validation that should be performed by the P-CSCF, IBCF and the S-CSCF.</p> <ul style="list-style-type: none"><li>• <b>Ingress SDP Offer:</b> Specifies whether P-CSCF/S-CSCF/IBCF validates SDP offer messages received from the external network.</li><li>• <b>Ingress SDP Answer:</b> Specifies whether P-CSCF/S-CSCF/IBCF validates SDP answer messages received from the external network.</li><li>• <b>Egress SDP Offer:</b> Specifies whether P-CSCF/S-CSCF/IBCF validates SDP offer messages sent to the external network.</li><li>• <b>Egress SDP Answer:</b> Specifies whether P-CSCF/S-CSCF/IBCF validates SDP answer messages sent to the external network.</li></ul> |

| Parameter                          | Provisioning   |
|------------------------------------|--|
| <b>Bandwidth Allowed Per Codec</b> | <p>Under <b>Bandwidth Allowed Per Codec</b>, Provision the following parameters:</p> <ul style="list-style-type: none"> <li>• Click <b>Add</b> to add all the allowed codecs along with their associated bandwidths.</li> </ul> <p><b>Result:</b> The <b>Bandwidth Configuration</b> window is displayed. This is used to save peak bandwidth and max burst size per codec type. In the <b>Bandwidth Configuration</b> window, provision the following parameters:</p> <ul style="list-style-type: none"> <li>– <b>Codec/Media Type</b></li> <li>– <b>Allowed Bandwidth</b></li> <li>– <b>Peak Bandwidth</b></li> <li>– <b>Max Burst Size</b></li> </ul> <p>Click <b>OK</b> once you have provisioned the parameters.</p> <ul style="list-style-type: none"> <li>• <b>Default Audio Codec Bandwidth</b> - Specifies the default bandwidth used for estimation of audio codec.</li> <li>• <b>Default Audio Codec Peak Bandwidth</b> - Specifies the default peak bandwidth used for estimation of audio codec.</li> <li>• <b>Default Audio Codec Max Burst Size</b> - Specifies the default max burst size used for estimation of audio codec.</li> <li>• <b>Default Video Codec Bandwidth</b> - Specifies the default bandwidth used for estimation of video codec.</li> <li>• <b>Default Video Codec Peak Bandwidth</b> - Specifies the default peak bandwidth used for estimation of video codec.</li> <li>• <b>Default Video Codec Max Burst Size</b> - Specifies the default max burst size used for estimation of video codec.</li> </ul> |
| <b>Audio Golden Codec Set</b>      | Under <b>Audio Golden Codec Set</b> , click <b>Add</b> to add all the allowed codecs.  |
| <b>Auxiliary Codec Set</b>         | Under <b>Auxiliary Codec Set</b> , click <b>Add</b> to add all the auxiliary codecs.   |

| Parameter                                    | Provisioning   |
|--|--|
| <b>VG Session BW Control</b>                 | <p>Under <b>VG Session BW Control</b>, provision the following parameters:</p> <ul style="list-style-type: none"> <li>• In the <b>Default Message Bandwidth</b> field, enter the maximum size of bandwidth to be allowed when the media type is message.</li> <li>• In the <b>Default Text Bandwidth</b> field, enter the maximum size of bandwidth to be allowed when the media type is text.</li> <li>• In the <b>Default Application Bandwidth</b> field, enter the maximum size of bandwidth to be allowed when the media type is an application.</li> </ul>   |
| <b>Bandwidth Allowed Per MSRP Media Type</b> | <p>Under <b>Bandwidth Allowed Per MSRP Media Type</b>,</p> <p>Provision the following parameters:</p> <ul style="list-style-type: none"> <li>• Click <b>Add</b> to add all the allowed media types along with their associated bandwidths. <b>Result:</b> The <b>Bandwidth Configuration</b> window is displayed. This is used to save maximum requested bandwidth allowed per MSRP media type in a SDP off/answer and the (optional) operator prescribed peak bandwidth and max burst size. In the <b>Bandwidth Configuration</b> window, provision the following parameters: <ul style="list-style-type: none"> <li>– <b>Codec/Media Type</b></li> <li>– <b>Allowed Bandwidth</b></li> <li>– <b>Peak Bandwidth</b></li> <li>– <b>Max Burst Size</b></li> </ul> </li> <li>• <b>Default MSRP Media Type Bandwidth</b> - Specifies the default bandwidth used for estimation of MSRP media type.</li> <li>• <b>Default MSRP Media Type Peak Bandwidth</b> - Specifies the default peak bandwidth used for estimation of MSRP media type.</li> <li>• <b>Default MSRP Media Type Max Burst Size</b> - Specifies the default max burst size used for estimation of MSRP media type.</li> </ul> |

| Parameter                   | Provisioning   |
|-----------------------------|--|
| <b>AMR Mode-Set Control</b> | <p>Under the <b>AMR Mode-Set Control</b> group, provision the following parameters:</p> <ul style="list-style-type: none"> <li>• Insert AMR-NB codec with Mode-set</li> <li>• Preferred AMR-NB mode-set</li> <li>• Insert AMR-WB codec with Mode-set</li> <li>• Preferred AMR-WB mode-set</li> <li>• Reuse SDP payload number if no mode-set in SDP offer</li> <li>• AMR preferred modeset priority</li> <li>• Mode Change Period</li> </ul> |

For more information on the parameters, see the topic **Session Description Protocol Profile** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

**6** Click **OK**.

**Result:** The Session Description Protocol Profile table attributes are provisioned successfully.

END OF STEPS

# To provision Service-Based PCSCF Profile

## Purpose

This procedure is used to provision Service-Based PCSCF Profiles. They define signaling compression and enforced access parameters.

## Steps to provision a Service-Based PCSCF Profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → PCSCF Tables**.

**Result:** The **PCSCF Tables** window is displayed.

- 2 In the left pane, expand the **Service-Based PCSCF Profile** folder.

**Result:** The Service-Based PCSCF Profile tables are listed under the folder in the left pane.

If the folder is empty, add a Service-Based PCSCF Profile table.

Perform the following steps in the **PCSCF Tables** window to add, rename, or delete a Service-Based PCSCF Profile table :

| If you want to ...                          | then ...  |
|---|---|
| add a Service-Based PCSCF Profile table,    | <ol style="list-style-type: none"><li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li><li>From the <b>Table Number</b> list, select the table number.</li><li>In the <b>Table Name</b> box, type a descriptive table name.</li><li>Click <b>OK</b>.</li></ol> <i>End of steps</i> |
| rename a Service-Based PCSCF Profile table, | <ol style="list-style-type: none"><li>Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li><li>In the <b>Table Name</b> box, type a new table name.</li><li>Click <b>OK</b>.</li></ol> <i>End of steps</i>   |

| If you want to ...                          | then ...   |
|---|--|
| delete a Service-Based PCSCF Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Service-Based PCSCF Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the Service-Based PCSCF Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **PCSCF Tables** window to provision the Service-Based PCSCF Profile table attributes:

| If you want to ...                                     | then ...  |
|--|---|
| add the Service-Based PCSCF Profile table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a Service-Based PCSCF Profile table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                                     | then ...  |
|--|---|
| delete a Service-Based PCSCF Profile table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.<br/><i>End of steps.</i></li> </ol>   |
| Enable compression,                                    | <p>Provision the following:</p> <ul style="list-style-type: none"> <li>• Select the <b>Compression Enabled</b> option. <b>Note:</b> The <b>Compression Enabled</b> option only affects outgoing message compression. Incoming message decompression is always active (if needed) and is <i>not</i> affected by this option.</li> <li>• In the <b>Enforced Access</b> area, specify for which access techniques compression should be enforced. <b>Note:</b> The <b>Enforced Access</b> selections, if any, are only used when screening incoming messages to ensure they are in a compressed (SigComp) format. Outgoing message compression is <i>not</i> affected by the selections.</li> <li>• Using the <b>Default Compressor</b> menu, select the default compression technique. <b>Note:</b> The <b>Default Compressor</b> selection only affects outgoing message compression. Incoming message decompression is always active (if needed) and is <i>not</i> affected by this selection.</li> </ul> |
| Disable compression,                                   | <p>Clear the <b>Compression Enabled</b> option. <b>Note:</b> The <b>Compression Enabled</b> option only affects outgoing message compression. Incoming message decompression is always active (if needed) and is <i>not</i> affected by this option.</p>  |

**5** Provision the following parameters:

| Parameter   | Provisioning  |
|---|---|
| <b>Heartbeat S-CSCF</b>   | <p>Select the <b>Yes</b> option for the <b>Heartbeat S-CSCF</b> parameter.</p> <p>This option enables the P-CSCF to perform the heartbeat operation to track the S-CSCF status.</p>   |
| <b>Tss Timer</b>  | <p>Retain the time duration in the <b>Tss Timer</b> field.</p> <p>This field defines the time duration between the heartbeat requests, sent to the S-CSCF which has responded to the previous request.</p>  |
| <b>Tsf Timer</b>  | <p>Retain the time duration in the <b>Tsf Timer</b> field.</p> <p>This field defines the time duration between the heartbeat requests, sent to the S-CSCF which has not responded, or which has not sent a success response to the previous request.</p>  |
| <b>Heartbeat Failure Threshold N</b>  | <p>Retain the value in the <b>Heartbeat Failure Threshold N</b> field.</p> <p>This field defines the number of consecutive heartbeat request attempts the S-CSCF has failed, before it is considered to have lost its registry. Recovery action is launched after the defined failed attempts.</p>          |
| <b>Maintain Call-ID/From tag for non-REGISTER request with challenge-response</b> | <p>Check the <b>Maintain Call-ID/From tag for non-REGISTER request with challenge-response</b> flag to control whether the originating PCSCF must maintain the same Call-ID and From tag for non-REGISTER request with challenge-response.</p> <p><b>Note:</b> The default value is <b>Not checked</b>.</p> |
| <b>TLS Profile ID</b>   | <p>Select the <b>TLS Profile ID</b>. This field indicates the relationship of a TLS profile with a specific IMS service.</p> <p><b>Note:</b> The default value is <b>None</b>. The values range from 1 to 64.</p>   |

| Parameter                 | Provisioning  |
|---------------------------|---|
| <b>As Secondary IBC</b>   | Select the check box to set the IBC to serve as secondary IBC.<br><br>It is also used to determine whether the 3GPP IBC performs the switchback handling or not.  |
| <b>IBC GR FQDN Domain</b> | Type the right most domain name of the 3GPP IBC GR FQDN that would be used if the IBC GR terminating request handling is expected. The 3GPP IBC GR FQDN has the format “GUL + ServiceLabel + IBC GR FQDN Domain”, and it is to be included in the registration request to the core network, and used for the terminating request routing. None indicates that no IBC GR FQDN Domain is provisioned. The primary and secondary IBC system must be configured to present the same 3GPP IBC GR FQDN. |

- 6 Click **OK**.

**Result:** The Service-Based PCSCF Profile table attributes are provisioned successfully.

END OF STEPS

# To provision SIP Stack Timer Profile

## Purpose

This procedure is used to provision an SIP Stack Timer Profile.

You can create up to 16 SIP Stack Timer Profiles. A default SIP Stack Timer Profile with Profile Id = 0 is created when the configuration host comes up if not already present.

## SIP Stack Timer Profile recommendations

Alcatel-Lucent recommends using of two SIP Stack Timer Profiles. The P-CSCF uses a specific default SIP Stack Timer Profile. A SIP Stack Timer Profile is used by all other components.

### Default SIP Stack Timer Profile for P-CSCF

The following table lists the recommended values for the default SIP Stack Timer Profile for the P-CSCF:

| Parameter                               | Recommended value |
|---|-------------------|
| T1                                      | 2000 ms           |
| T2                                      | 16 sec            |
| T4                                      | 17 sec            |
| C                                       | 180 sec           |
| INVITE Fast Transaction Guard Timer     | $4 * T1$          |
| Non INVITE Fast Transaction Guard Timer | $9 * T1$          |

### SIP Stack Timer Profile for all other components except P-CSCF

The following table lists the recommended values for the SIP Stack Timer Profile:

| Parameter                               | Recommended value |
|---|-------------------|
| T1                                      | 500 ms            |
| T2                                      | 4 sec             |
| T4                                      | 5 sec             |
| C                                       | 180 sec           |
| INVITE Fast Transaction Guard Timer     | $4 * T1$          |
| Non INVITE Fast Transaction Guard Timer | $9 * T1$          |

## Before you begin

Observe the following:

- The P-CSCF must be available in the network.

### Frequency

This procedure must be performed per P-CSCF.

### System requirements

Provisioning GUI connection.

## Steps to provision a SIP Stack Timer Profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Tables**.

**Result:** The **IMS Tables** window is displayed.

- 2 In the left pane, expand the **IMS → General → SIP Stack Timer Profile** folder.

**Result:** The SIP Stack Timer Profiles tables are listed under the folder in the left pane.

If the folder is empty, add a SIP Stack Timer Profile table.

Perform the following steps in the **IMS Tables** window to add, rename, or delete a SIP Stack Timer Profile table :

| If you want to ...                   | then ...  |
|--------------------------------------|---|
| add a SIP Stack Timer Profile table, | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>IMS Tables</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <i>End of steps</i> |

| If you want to ...                      | then ...   |
|---|--|
| rename a SIP Stack Timer Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>IMS Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>       |
| delete a SIP Stack Timer Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a SIP Stack Timer Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

**3** Click **OK**.

**Result:** The SIP Stack Timer Profile table attributes are provisioned successfully.

END OF STEPS

## To provision PCSCF profile

### Purpose

This procedure is used to add, modify, or delete a PCSCF Profile. The maximum number of PCSCF Profiles that can be created is 2048.

### When you *add* a PCSCF Profile table

When you *add* a new PCSCF Profile table, the table is empty.

### Before you *delete* a PCSCF Profile table

Before you *delete* a PCSCF Profile table, ensure that the profile is NOT used by an SIPia port.

### Steps to provision a PCSCF Profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → PCSCF Tables**.

**Result:** The **PCSCF Tables** window is displayed.

- 2 In the left pane, expand the **PCSCF Profile** folder.

**Result:** The PCSCF Profile tables are listed under the folder in the left pane.

If the folder is empty, add a PCSCF Profile table.

Perform the following steps in the **PCSCF Tables** window to add, rename, or delete a PCSCF Profile table :

| If you want to ...         | then ...   |
|----------------------------|--|
| add a PCSCF Profile table, | <ol style="list-style-type: none"><li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li><li>From the <b>Table Number</b> list, select the table number.</li><li>In the <b>Table Name</b> box, type a descriptive table name.</li><li>Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |

| If you want to ...            | then ...  |
|-------------------------------|---|
| rename a PCSCF Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a PCSCF Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a PCSCF Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>    |

- 3 Double-click the table to open the list of profiles defined for the table.  
Add the PCSCF Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.
- 4 Perform the following steps at the **PCSCF Tables** window to add, modify, or delete the PCSCF Profile table attributes:

| If you want to ...                      | then ...  |
|---|---|
| add the PCSCF Profile table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                       | then ...   |
|--|--|
| modify a PCSCF Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a PCSCF Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>            |

**5** Provision the following parameters:

| Parameter                  | Provisioning  |
|----------------------------|---|
| <b>PCSCF Profile Id</b>    | Enter a unique number to identify the profile in the <b>PCSCF Profile Id</b> field. |
| <b>Profile Description</b> | Enter a brief description in the <b>Profile Description</b> field.                  |

| Parameter                              | Provisioning   |
|--|--|
| <b>Provide P-CSCF IP Address to UE</b> | <p>Select the <b>Provide P-CSCF IP Address to UE</b> check box to specify the IP address and port number of the P-CSCF (instead of the P-CSCF FQDN) in the SIP message headers sent to the UE.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>Before selecting this field, ensure that the <b>Enable Two NIs for SIP</b> check box is selected in the SIPia port configured to this PCSCF Profile.</li> <li>The <b>SIP Header Reduction</b> option takes higher priority compared to the <b>Provide P-CSCF IP Address to UE</b> option. This means that when the <b>SIP header reduction</b> check box is selected, the Record-Route header is erased from the messages in the SUBSCRIBE/REFER dialog which are sent to the UE.</li> </ul> |
| <b>Network Indicator</b>               | Enter the <b>Network Indicator</b> to define the Proxy Call Session Control Function (P-CSCF) URI.   |
| <b>ACR Charging Profile ID</b>         | <p><b>Note:</b> ACR Charging Profile with ID 0 is regarded as a default profile. The default profile is mapped to 3GPP version 8 ACR messages. The content of default profile is not changeable through the FS GUI. If the P-CSCF is correlated to default profile and the version needs to be changed, you can add a new ACR charging profile with the expected version selection and associate the P-CSCF to the new ACR charging profile.</p> <p>Select the ACR Charging Profile ID to which the P-CSCF needs to be mapped in the <b>ACR Charging Profile ID</b> list.</p>  |
| <b>SIP Stack Timer Profile Id</b>      | Select the non-default <b>SIP Stack Timer Profile Id</b> with values for the P-CSCF.   |
| <b>Published Realm</b>                 | <p>Select a realm from the <b>Published Realm</b> list.</p> <p>To provision a published realm, see “<a href="#">To provision a Published Realm</a>” (p. 4-286).</p>  |

| Parameter                                     | Provisioning  |
|---|---|
| <b>Support Outbound Keep-Alive Mechanisms</b> | <p>Select the <b>Yes</b> button of the <b>Support Outbound Keep-Alive Mechanisms</b> field to support STUN and TCP outbound keep-alive mechanisms.</p> <p><b>Note:</b> The Symmetric TCP Connections flag must be set to any value other than Off (for example, <b>FW/NAT or SIP Outbound</b> or <b>Always</b>) when the <b>Support Outbound Keep-Alive Mechanisms</b> check box is selected.</p>                               |
| <b>Use P-Asserted-Identity Header</b>         | <p>Retain <b>No</b> in the <b>Use P-Asserted-Identity Header</b> field to remove the P-Asserted-Identity headers from the SIP requests/responses exchanged with the UE/PBX.</p>   |
| <b>Remove Untrusted Headers</b>               | <p>Retain <b>Yes</b> in the <b>Remove Untrusted Headers</b> field to remove the headers which must be exchanged only with trusted entities, in the SIP requests/responses.</p>  |
| <b>Close Signaling Connection to UE</b>       | <p>Select the <b>Close Signaling Connection to UE</b> check box. This flag determines whether the P-CSCF must close the TCP SIP signaling connection to the UE, when it detects the UE's loss of signaling path.</p>  |
| <b>Registration Suppression Enabled</b>       | <p>Select the <b>Registration Suppression Enabled</b> check box. This flag is used to enable or disable the Registration Suppression capability.</p> <p>If the UE is not behind NAT, the value in the “expires” parameter of the Contact header is populated from “P-CSCF Registration Interval to UE”.</p> <p>If UE is behind NAT, the “expires” header is populated from “P-CSCF Registration Interval to UE behind NAT”.</p> |

| Parameter  | Provisioning  |
|--|---|
| <b>Apply Registration Suppression only when NAT detected</b> | Select the <b>Apply Registration Suppression only when NAT detected</b> check box. This flag determines whether the Registration Suppression capability (if enabled) is applied to all endpoints (when set to No) or only to the endpoints for which far-end NAT is detected (when set to Yes). The value for the “expires” parameter of the Contact header is populated from “P-CSCF Registration Interval to UE behind NAT”.  |
| <b>PCSCF Registration Interval for UE</b>                    | Enter the value in the <b>PCSCF Registration Interval for UE</b> box. The value can range from 30 to 3600. This field defines the PCSCF Registration Interval for UE and applies only to UEs that are not behind far-end NAT.   |
| <b>PCSCF Registration Interval for UE behind NAT (secs)</b>  | <p>Enter the value in the <b>PCSCF Registration Interval for UE behind NAT (secs)</b> box. This determines the value of the “expires” parameter of the Contact header that is reported to the UE (behind NAT) in the 200 OK to REGISTER for both initial and reregisters cases. This value applies only to the UE that is behind far-end NAT.</p> <p>When <b>Apply Registration Suppression only when NAT detected</b> is disabled, this field specifies the value sent in the Expires header or the “expires” parameter in Contact header for UE behind NAT and <b>P-CSCF Registration for UE</b> specifies the value sent in the Expires header or the “expires” parameter in Contact header for UE not behind NAT.</p> <p><b>Note:</b> The value must be set and is only used when <b>Registration Suppression Enabled</b> field is enabled.</p> |

| Parameter  | Provisioning   |
|--|--|
| <b>Backoff Interval for Improper REGISTER</b>              | <p>Enter a value in the <b>Backoff Interval for Improper REGISTER</b> field.</p> <p>When 403 is sent as a reply to the initial REGISTER request of a user agent, you encounter situations such as user agent ignoring the 403 message and repeatedly sending initial REGISTER requests. The value in the <b>Backoff Interval for Improper REGISTER</b> field is used as the registration interval that is specified in the 200 OK message, sent by the P-CSCF to the user agent. This serves the purpose of delaying the initial REGISTER requests from the user agent.</p>  |
| <b>Registration Interval Override towards SCSCF (secs)</b> | <p>Enter a value in the <b>Registration Interval Override towards SCSCF (secs)</b> field.</p> <p><b>Note:</b> When this field is non-zero ( minimum of 300 seconds registration interval to align with S-CSCF), the P-CSCF overwrites the UE provided non-zero registration interval in a REGISTER request with the configured value for the P-CSCF before sending the REGISTER request to the S-CSCF.</p>   |
| <b>Default PANI</b>  | <p>For Internet users, populate the <b>Default PANI</b> field. The default value of <b>Default PANI</b> is NULL. Now the <b>Support 3GPP/TISPAN Emergency Calls</b> in the <b>Miscellaneous Parameters</b> tab cannot be checked.</p> <p>Refer to "<a href="#">To provision an E-CSCF Profile table</a>" (p. 4-212) for more information.</p> <p>E-CSCF profile is used to choose the Emergency Session Routing Methods.</p> <p>SFR-LRF is one of the Emergency Session Routing Methods.</p> <p><b>Note:</b> The fields <b>Default PANI</b> and <b>Domain Name for PANI</b> cannot be provisioned at the same time. If the field <b>Domain Name for PANI</b> is provisioned, then the field <b>Default PANI</b> must be blank.</p> |

| Parameter                        | Provisioning  |
|----------------------------------|---|
| <b>SIP Topology Hiding</b>       | <p>To enable the P-CSCF to hide network topology information in the SIP messages exchanged over the Gm interface, select the <b>SIP Topology Hiding</b> check box.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• To modify this field, ensure that all the P-CSCF SIPia ports using this profile are out of service.</li> <li>• Ensure that a valid value is provided in the <b>Topology Hiding Host String</b> field, in the NGSS parameters screen.</li> </ul> |
| <b>Symmetric TCP Connections</b> | <p>Select any value other than <b>OFF</b> in the <b>Symmetric TCP Connections</b> list to support outbound STUN and TCP outbound keep-alive mechanisms.</p>   |
| <b>Security Parameters</b>       | <p>Click <b>Security Parameters</b> tab.</p>  |

| Parameter                          | Provisioning   |
|------------------------------------|--|
| <b>Security Gateway Profile Id</b> | <p>To apply the Security Gateway, select the required profile in the <b>Security Gateway Profile Id</b> drop-down box.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• To activate the Security Gateway function, ensure that the <b>Enable Two NIs for SIP</b> check box is selected in the <b>General Parameters</b> tab.</li> <li>• In the Signaling Firewall scenario: <ul style="list-style-type: none"> <li>– If <b>Security Gateway Profile Id</b> is zero, all P-CSCF SIPia ports using this profile record must reside on IMS services that are FEPH disabled. In this case, the P-CSCF is not protected by the Security Gateway or by the Signaling Firewall.</li> <li>– If <b>Security Gateway Profile Id</b> is non-zero and the <b>Security Gateway Profile Id</b> record does not have the FEPH Policy Ids specified, all P-CSCF SIPia ports using this profile record must reside on IMS services that are FEPH disabled. In this case the P-CSCF is protected by the Security Gateway.</li> <li>– If <b>Security Gateway Profile Id</b> is non-zero and the <b>Security Gateway Profile Id</b> record has FEPH Policy Ids specified, all PCSCF SIPia ports using this profile record must reside on IMS services that are FEPH enabled. In this case the P-CSCF is protected both by the Security Gateway and by FEPH.</li> </ul> </li> </ul> |
| <b>Enable IP association</b>       | <p>To enable the P-CSCF to use IP association to assert calling party identity, select the <b>Enable IP association</b> check box.</p> <p><b>Note:</b> To enable the “P-CSCF support of calling party ID assertion using IP association” feature follow the procedure in the topic, <i>“P-CSCF support of calling party ID assertion using IP association” in the ISC Application User Guide.</i></p>  |

| Parameter  | Provisioning   |
|--|--|
| <b>Populate P-Asserted-Identity When Only From Header is Present</b> | <p>Select the necessary option in the <b>Populate P-Asserted-Identity When Only From Header is Present</b> drop-down box.</p> <ul style="list-style-type: none"> <li>• <b>Use From</b> option indicates that the From header is used to populate PAID, when PAID and P-Preferred-Identity do not exist in the received message.</li> <li>• <b>Use Default</b> indicates that the default PUID is used to populate PAID.</li> </ul>   |
| <b>IP Association Source Granularity</b>                             | <p>Select the source granularity for the IP association in the <b>IP Association Source Granularity</b> drop-down box.</p>   |
| <b>TLS Mandatory (Gm Only)</b>                                       | <p>Enable <b>TLS Mandatory (Gm Only)</b> for P-CSCF to validate that termination and origination is for TLS only.</p>  |
| <b>Interface Supports TLS</b>  | <p>Select the appropriate option from the <b>Interface Supports TLS</b> list.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>• <b>None</b> - If this option is selected then the SIP over TLS is not supported on Gm or Mw.</li> <li>• <b>Gm only</b> - If this option is selected then the SIP over TLS is supported on Gm interface but not supported on Mw interface.</li> <li>• <b>Gm+Mw</b> - If this option is selected then the SIP over TLS is supported on Gm and Mw interfaces. This option can be selected only when the <b>SIP Topology Hiding</b> check box on the <b>General Parameters</b> tab of PCSCF Profile is enabled.</li> </ul> <p><b>Note:</b> When the TLS server port number for a P-CSCF is set to non-zero, then there will be a cross check to ensure that this parameter is set to Gm or Gm+Mw.</p> |

| Parameter                           | Provisioning  |
|-------------------------------------|---|
| <b>Convert SIPS URI</b>             | <p>Enable the <b>Convert SIPS URI</b> check box.</p> <p>This check box can only be enabled when the following conditions are met:</p> <ul style="list-style-type: none"> <li>• PCSCF Profile mapping to one P-CSCF SIPia port with non zero valid TLS server port (like 5061)</li> <li>• The <b>Interfaces Supports TLS</b> field is set to Gm only.</li> <li>• The <b>SIP Topology Hiding</b> check box on the <b>General Parameter</b> tab is enabled.</li> </ul>   |
| <b>IBC Configuration Parameters</b> | <p>Under <b>IBC Configuration Parameters</b>, do the following:</p> <ul style="list-style-type: none"> <li>• From the <b>IBC-Access Mode</b> list, select the IBC access mode.<br/>The available options:             <ul style="list-style-type: none"> <li>– 3GPP P-CSCF</li> <li>– Non-3GPP IBC</li> <li>– 3GPP IBC</li> </ul> </li> <li>• From the IBC-A Profile list, select the IBC profile ID.</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• When IBC-Access Mode is set to 3GPP IBC or Non-3GPP IBC, IBC-A Profile ID must be nonzero. When IBC-Access Mode is set to 3GPP PCSCF, IBC-A Profile ID can be either zero or non-zero.</li> <li>• When IBC-Access Mode is set to 3GPP IBC or Non-3GPP IBC, SIP Topology Hiding must be enabled.</li> <li>• If the PCSCF Port is using a profile with IBC Access Mode set to 3GPP IBC or Non-3GPP IBC, then <b>Enable Two NIls for SIP</b> must be set to Yes.</li> <li>• If a PCSCF Profile is referencing both IBC-A Profile and Published Realm, then "IP Version to Provide to Access" in IBC-A Profile should be consistent with "IP Version" in Published Realm (that is, either same IP version or that Published Realm indicates both).</li> </ul> |

| Parameter   | Provisioning  |
|---|---|
| <b>ATCF Configuration Parameters</b>              | <p>Go to <b>ATCF Configuration Parameters</b> tab and select <b>Yes</b> in the <b>Support ATCF</b> option to enable support for ATCF functionality.</p> <p>The <b>Support ATCF</b> field is allowed to be enabled only if:</p> <ul style="list-style-type: none"> <li>• <b>Enable Two NI's for SIP</b> is set to 'Yes' on the SIPia port profile that is using this Profile.</li> <li>• SBLP support is enabled and a SBLP Profile is assigned that has the Diameter Interface Type set to '3GPP/TISPAN'.</li> <li>• Gq' and Rx interfaces are enabled for the P-CSCF/ATCF.</li> </ul> <p>The P-CSCF SIPia port does not allow the user to disable "Support for 2 NI's" if the PCSCF Profile for the given port has <b>Support ATCF</b> enabled (set to Yes).</p> |
| <b>Policy to Include ATCF</b>                     | <p>Under the <b>Policy to Include ATCF</b> list, select the value, <b>Always Include ATCF</b>.</p> <p>This field defines when the ATCF is to include itself in the Path header during UE Registration. This field can be enabled only when the <b>Support ATCF</b> option is set to <b>Yes</b>.</p>   |
| <b>Policy to Include ATGW</b>                     | <p>Under the <b>Policy to Include ATGW</b> list, select the value, <b>Always Include ATGW</b>.</p> <p>This field defines the conditions under which the ATCF invokes the ATGW during Session setup for media anchoring. This field can be enabled only when the <b>Support ATCF</b> option is set to <b>Yes</b>.</p>  |
| <b>Policy for Media Transcoding During eSRVCC</b> | <p>Under the <b>Policy for Media Transcoding During eSRVCC</b> list, select the appropriate value.</p> <p>The default value is <b>Perform Transcoding Locally</b>.</p> <p>This field defines how transcoding should be performed. This field can be enabled only when the <b>Support ATCF</b> option is set to <b>Yes</b>.</p>  |

| Parameter  | Provisioning   |
|--|--|
| <b>Wait for Possible eSRVCC Before Call Clearing Timer</b> | <p>Enter the appropriate value in the <b>Wait for Possible eSRVCC Before Call Clearing Timer</b> field.</p> <p>The default value is 8 secs.</p> <p>The ATCF waits for this period of time before sending BYE towards S-CSCF to clear the source access leg after it receives a ASR or RTR from PCRF with Abort_Cause = “PS_TO_CS_HANDOVER”. This timer is only applicable for a P-CSCF with ATCF enabled. In other words, this field can be enabled only when the <b>Support ATCF</b> option is set to <b>Yes</b>.</p> |
| <b>Send ACR For HO Request</b>                             | <p>Select the <b>Send ACR For HO Request</b> check box.</p> <p>This field defines whether the P-CSCF needs to send ACR for HO request. This field can be enabled only when the <b>Support ATCF</b> option is set to <b>Yes</b>.</p>  |
| <b>Send BYE to UE to Release Source Access Leg</b>         | <p>Select the <b>Send BYE to UE to Release Source Access Leg</b> check box.</p> <p>This field defines if BYE message needs to be sent to the UE to release the source access leg after successful HO. This field can be enabled only when the <b>Support ATCF</b> option is set to <b>Yes</b>.</p>   |

| Parameter   | Provisioning   |
|---|--|
| <b>Miscellaneous Parameters</b>                       | <p>Go to <b>Miscellaneous Parameters</b> tab of P-CSCF and select <b>Yes</b> in the <b>Support 3GPP/TISPAN Emergency Calls</b> field to support emergency calls. The Emergency Identifiers list must be populated before setting <b>Support 3GPP/TISPAN Emergency Calls</b> to <b>Yes</b>.</p> <p><b>Note :</b> If the E-CSCF profile is provisioned to support 3GPP and TISPAN standards, assign an IMS Emergency Service Identifier table to E-CSCF. The Emergency Identifiers List is provisioned for the P-CSCF to identify if the incoming call is an emergency call. If SFR-LRF is the ESRM there would be need to support up to 40 emergency identifiers.</p> <p>For more information, see “<a href="#">To provision IMS Emergency Service Identifier</a>” (p. 4-208) .</p> |
| <b>Emergency Host URI</b>                             | <p>Enter the emergency host URI in the <b>Emergency Host URI</b> field.</p>  |
| <b>R-URI to Emergency Host</b>                        | <p>Enter the Request-URI to the emergency host in the <b>R-URI to Emergency Host</b> field.</p> <p>This field is optional and can be provisioned with a valid URI (For example, sip:+911@ims.lucentlab.com) or a null string when the <b>Support 3Gpp/TISPAN emergency calls</b> field is set to <b>Yes</b>.</p> <p>The P-CSCF replaces the R-URI of the outgoing INVITE for 3gpp emergency calls with the <b>R-URI to Emergency Host</b>, if it is provisioned. If this field is not provisioned (if it is a null string), then the P-CSCF will not replace the R-URI of the outgoing INVITE for 3gpp emergency calls.</p>  |
| <b>Support Emergency Calls for Unregistered Users</b> | <p>Select <b>Yes</b> in the <b>Support Emergency Calls for Unregistered Users</b> field to support emergency calls for unregistered users.</p>   |

| Parameter   | Provisioning   |
|---|--|
| <b>XML Body in 380</b>                            | <p>Select the option <b>Yes</b> in the <b>XML Body in 380</b> field, in order to include xml body in the 380 response.</p> <p>If you select <b>No</b>, then the xml body will not be included in the 380 response.</p>   |
| <b>Miscellaneous Parameters</b>                   | <p>If SFR-LRF is the ESRM, go to <b>Miscellaneous Parameters</b> tab of P-CSCF and in the <b>TISPAN e2 Parameters</b> group, and select <b>Use-IP for Support TISPAN e2 Interface</b> between P-CSCF and the Connectivity session Location and repository Function (CLF).</p> <p><b>Note:</b> When <b>Support for TISPAN e2 Interface</b> is enabled, <b>IP Address Realm</b>, and <b>Application Function Identifier</b> must be provisioned, and <b>Remove P-Access-Network-Info</b> should be set to <b>Yes</b>.</p>  |
| <b>CLF e2 Query for Unregistered Users</b>        | <p>Select <b>Yes</b> in the <b>CLF e2 Query for Unregistered Users</b> field to support TISPAN e2 interface between P-CSCF and the Connectivity session Location and repository Function (CLF).</p> <p><b>Note:</b> If the <b>Domain Name for PANI</b> field is provisioned then the TISPAN e2 must be disabled.</p>   |
| <b>Reason for 380 Redirection</b>                 | <p>Enter the reason for 380 redirection in the <b>Reason for 380 Redirection</b> field.</p>  |
| <b>Insert Priority Header for Emergency Calls</b> | <p>Select the <b>Insert Priority Header for Emergency Calls</b> check box. This field provides an option to include Priority: emergency in requests identified as emergency calls.</p> <ul style="list-style-type: none"> <li>• If this option is not checked, P-CSCF does not react</li> <li>• If this option is checked and it is not an emergency INVITE, P-CSCF does not react</li> <li>• If this option is checked and it is an emergency INVITE, P-CSCF removes the received Priority header, and inserts a Priority header with "emergency" parameter.</li> </ul> |

| Parameter             | Provisioning  |
|-----------------------|---|
| <b>SIP Filter Set</b> | Select an SIP filter set from the <b>SIP Filter Set</b> list. This SIP filter set is used to screen the SIP messages that pass through the P-CSCF from or to the access network.  |
| <b>Access Type</b>    | <p>Select the appropriate value from the <b>Access Type</b> list.</p> <p><b>Note :</b> The <b>Domain Name for PANI</b> field is blank if the <b>Access Type</b> value is set to DOCSIS, 3GPP-E-UTRAN-TDD, or 3GPP-E-UTRAN-FDD. If the SBC domain name is provisioned and the administrator changes the <b>Access Type</b> value to DOCSIS, 3GPP-E-UTRAN-TDD, or 3GPP-E-UTRAN-FDD, then the provisioned SBC domain name is erased.</p> |
| <b>Country Code</b>   | <p>Enter the appropriate value in the <b>Country Code</b> field.</p> <p>This field specifies the Country Code supported for the P-CSCF instance.</p> <p>The allowed digit range in the <b>Country Code</b> field is 1 to 3 digits.</p>  |
| <b>Area Code</b>      | <p>Enter the appropriate value in the <b>Area Code</b> field.</p> <p>This field specifies the Area Code supported for the P-CSCF instance.</p> <p>The allowed digit range in the <b>Area Code</b> field is 1 to 4 digits.</p>   |

| Parameter                                    | Provisioning   |
|--|--|
| <b>Domain Name for PANI</b>                  | <p>Enter the appropriate value in the <b>Domain Name for PANI</b> field.</p> <p>This field specifies the Domain Name for the P-CSCF instance.</p> <p>The maximum allowed characters are 100 and the allowed characters are 0-9, a-z, A-Z, “.” and “-”.</p> <p>When an SIP request (non-REGISTER SIP request) is received and a domain name is provisioned, PCSCF removes all received PANI header(s) and inserts a network provided PANI header with a string defined as follows: PANI header must contain the src ip and udp port of the GW from which it got registered. For 3GPP emergency calls (P-CSCF routes them to E-CSCF directly), the E-CSCF extracts a domain name from the received PANI header based on the global provisioning parameter (domain type of PANI) setting. The E-CSCF uses the received domain name to obtain a default access location if the IP and port of the UE is not defined in the IP mapping table. The default access location can map to an emergency service routing number which the E-CSCF uses to route the INVITE out.</p> |
| <b>Common Announcement Module(CANM) Data</b> | <p>In the <b>Common Announcement Module(CANM) Data</b> group, select the appropriate value from the <b>CANM URI</b> list.</p> <p>This parameter defines the Common Announcement Module URI that is provisioned for a component that needs to send requests to the CANM to play an announcement on behalf of the component.</p>   |
| <b>Support P-Served-User Header</b>          | <p>When enabled, the <b>Support P-Served-User Header</b> option controls whether P-CSCF supports P-Served-User Header, and sends it to SCSCF in SIP request.</p>   |

| Parameter  | Provisioning   |
|--|--|
| <b>Support Interworking with Edge Network Providing Diversion Services</b> | <p><b>Support Interworking with Edge Network Providing Diversion Services</b> option controls the preference given to the specified header when generating PServed- User header.</p> <p>If History-Info header is present, convert to P-Served-User header; otherwise, if Diversion header is present, convert to P-Served-User header; if none of them is present, do not generate PServed- User.</p> <p>If Diversion header is present, convert to P-Served-User header; otherwise, if History-Info header is present, convert to P-Served-User header; if none of them is present, do not generate PServed- User.</p> <p>None: Do not convert History-Info or Diversion header to P-Served-User header.</p> |
| <b>SIP Error Treatment Table</b>   | <p>To set the SIP Error Treatment Table ID referred by this profile, select a valid table ID from the <b>SIP Error Treatment Table</b> list.</p>   |
| <b>SIP Heartbeat After INVITE failure on Gm Interface</b>                  | <p>This configuration field determines if the HB is sent to Gm interface. By default, most Gm interfaces are used to connect to UEs. These type of links are not usually monitored. However, in the case of PBX, IBC or BAC connections, they may appear as Gm interface, and it is useful to monitor them.</p> <p>This field can only be enabled if Support SIP Heartbeat after INVITE failure feature (per PCSCF component) is enabled and if the current P-CSCF profile is being used by P-CSCF SIPia port.</p>   |

| Parameter  | Provisioning  |
|--|---|
|  <b>Service-URN</b> | <p>The Service-URN is used to populate the Service-URN AVP (type OctetString) in the AAR message, and it indicates that an AF session is used for emergency traffic.</p> <p>The following are a few examples of the valid values of the AVP:</p> <ul style="list-style-type: none"><li>• <b>sos.emergency</b> - Emergency services</li><li>• <b>sos.ambulance</b> - Ambulance service</li><li>• <b>sos.animal control</b> - Animal control</li><li>• <b>sos.fire</b> - Fire service</li><li>• <b>sos.gas</b> - Gas leaks</li><li>• <b>sos.marine</b> - Maritime search and rescue</li><li>• <b>sos.mountain</b> - Mountain rescue</li><li>• <b>sos.physician</b> - Physician referral service</li><li>• <b>sos.poison</b> - Poison control center</li><li>• <b>sos.police</b> - Police, law enforcement</li></ul> |

For more information on the parameters, see the topic **Pcscf Profile Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

6 Click OK.

**Result:** The PCSCF Profile table attributes are provisioned successfully.

END OF STEPS

# To provision PBX Table Entry

## Overview

This procedure is used to provision a PBX Table Entry.

PBX Table is introduced in the Provision GUI to provide all the information that is required by P-CSCF to perform surrogate registration. Totally, 2048 PBX tables exist, and a maximum of 4096 of PBX entries that are allowed per system.

## Steps to provision a PBX Table Entry

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **PCSCF Tables**.

**Result:** The **PCSCF Tables** window is displayed.

- 2 In the left pane, expand the **PBX Table Entry** folder.

**Result:** The PBX Table Entry tables are listed under the folder in the left pane.

If the folder is empty, add a PBX Table Entry.

Perform the following steps in the **PCSCF Tables** window to add, rename, or delete a PBX Table Entry :

| If you want to ...     | then ...   |
|------------------------|--|
| add a PBX Table Entry, | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...        | then ...  |
|---------------------------|---|
| rename a PBX Table Entry, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a PBX Table Entry, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a PBX Table Entry, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>        |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the PBX Table Entry profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **PCSCF Tables** window to add, modify, or delete the PBX Table Entry attributes:

| If you want to ...                  | then ...  |
|-------------------------------------|---|
| add the PBX Table Entry attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                   | then ...   |
|--------------------------------------|--|
| modify a PBX Table Entry attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a PBX Table Entry attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                |

## 5 Provision the following parameters:

| Parameter                    | Provisioning   |
|------------------------------|--|
| <b>PBX Record ID</b>         | Select a <b>Record ID</b> for the PBX in the <b>PBX Record ID</b> field. This record ID must be unique per office.   |
| <b>PBX Name</b>              | Enter a descriptive text to name the PBX in the <b>PBX Name</b> field. The range for this name must be within 64 characters.   |
| <b>State</b>                 | The <b>State</b> field is disabled by default. If you change <b>State</b> from <b>Enable</b> to <b>Disable</b> , P-CSCF performs surrogate registration for the PBX.   |
| <b>PBX PrID</b>              | Enter a PBX Private User ID in the <b>PBX PrID</b> field. This ID should have a maximum of 256 characters only.  |
| <b>Authentication Scheme</b> | The <b>Authentication Scheme</b> parameter allows you to authenticate surrogate registration. From the menu, you can select <b>No Authentication</b> or <b>Digest MD5</b> . Specify the value for <b>Authentication Scheme</b> . |

| Parameter                    | Provisioning  |
|------------------------------|---|
| <b>Authentication Data</b>   | If you have selected <b>Digest MD5</b> in the previous step, then the <b>Authentication Data</b> allows you to save password. Passwords must be encrypted locally.  |
| <b>PBX PUID User</b>         | The <b>PBX PUID User</b> and <b>PBX PUID Host</b> information is used by P-CSCF to construct pbxPUID in SIP URI format: Sip:user@host   |
| <b>Registrar Name</b>        | Enter the <b>Registrar Name</b> information. This information is used by P-CSCF to construct the Request URI for REGISTER request. If you do not define this field, P-CSCF uses the pbxPUID-host to construct the Request-URI for REGISTER request.   |
| <b>PBX Contact Host</b>      | Enter the <b>PBX Contact Host</b> information. The host must have a maximum of 256 characters only.<br><br>The format of <b>PBX Contact Host</b> is FQDN, FQDN:port, <IP>, or <IP:Port>. The value ranges from 0 to 65535.  |
| <b>PBX Contact User</b>      | Enter the <b>PBX Contact User</b> information. This information is used by P-CSCF to construct the Contact header in REGISTER request in SIP URI format: Sip:[pbx-contact-user]@pbxcontacthost;[ transport=]. Must have a maximum of 64 characters only.  |
| <b>PBX Contact Parameter</b> | Enter the <b>PBX Contact Parameter</b> information. This field defines additional Contact header parameters that you want to include in the Contact header of REGISTER. For example, q=0.7.<br><br><b>Note:</b> “expires=” is also a Contact header parameter, but defined in <b>Register Expire Timer (sec)</b> field. |
| <b>PBX Contact Transport</b> | Enter the <b>PBX Contact Transport</b> information. If UDP or TCP is specified, a “transport =” the specified parameter is included in the Contact header for REGISTER request.   |

| Parameter                     | Provisioning  |
|-------------------------------|---|
| <b>Register Expire Timer</b>  | Enter the <b>Register Expire Timer</b> information. P-CSCF uses this information to populate the <b>expires</b> parameter in Contact header of REGISTER request.  |
| <b>Permanent Link Set</b>     | The <b>Permanent Link Set</b> field is disabled by default. If enabled, the P-CSCF establishes PLS toward the PBX and starts heartbeat.   |
| <b>Max Register Attempt</b>   | Enter the <b>Max Register Attempt</b> information as required.<br><br>This field defines the number of times a P-CSCF attempts surrogate registration for a PBX, if the previous attempt fails. Value ranges from 0 to 10. 0 refers to unlimited attempts.<br><br><b>Attention:</b> This parameter will be supported in future releases. The P-CSCF continues trying to register in this release. |
| <b>Register Retry Timer</b>   | Enter the <b>Register Retry Timer</b> information as required.<br><br>This field defines how long P-CSCF must wait before attempting another register, if the previous attempt fails. Value ranges from 30-3600 seconds. The default value is 300.  |
| <b>Max Attempt Per Minute</b> | Enter the <b>Max Attempt Per Minute</b> information as required. This field defines the number of times in a minute the P-CSCF attempts to send REGISTER request in response to the 401 authentication challenge.   |

For more information on the parameters, see the topic **Pbx ProfileTable** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The PBX Table Entry attributes are provisioned successfully.

END OF STEPS

---

# To activate the SIP header reduction

## Overview

This procedure is used to activate the SIP header reduction. This feature is used to reduce the number of headers sent to the end points.

## Procedure

Perform the following at the Provisioning GUI:

- 
- 1 Select **IMS → IMS Components → PCSCF Tables**.
- 

- 2 In the left pane, expand the **PCSCF Profile**.
- 

- 3 Right-click on the profile and select **Open** from the menu to open the table.
- 

- 4 Select an entry, right-click, and select **Modify Table Attributes**.

**Result:** The **PCSCF Profile Attribute** window displays.

---

- 5 Select the **SIP Header Reduction** check box.
- 

- 6 Click **OK**.

**Result:** The SIP header reduction is activated.

END OF STEPS

---

# To activate Service Route header

## Purpose

This topic describes the procedure to activate the Service Route header (for non-IPSec enabled UE) on a P-CSCF profile. After activation, the P-CSCF can either insert or remove the Service Route header from the 200 OK message that is sent to a UE to indicate a successful registration.

## Before you begin

Observe the following:

- The P-CSCF must be available in the network.
- This procedure must be performed for each P-CSCF.

## Procedure

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → PCSCF Tables**.
- 2 In the left pane, expand the **PCSCF Profile** table group.
- 3 Select and double click on the specific PCSCF Profile table. Right-click the desired entry and select **Attributes → Modify Table Attributes** from the menu.  
**Result:** The **PCSCF Profile Attributes** window displays.
- 4 In the **General Parameters** tab:

| If you want to...             | then...   |
|-------------------------------|---|
| enable Service Route header,  | check the <b>PCSCF in Service Route</b> check box.<br><i>End of procedure</i> |
| disable Service Route header, | clear the <b>PCSCF in Service Route</b> check box.<br><i>End of procedure</i> |

- 5 Click **OK**.

**Result:** The new values are updated.

END OF STEPS

# To activate PacketCable authentication in the P-CSCF profile

## Purpose

This topic contains the procedure to activate PacketCable authentication on a P-CSCF profile.

**Note:** Once the P-CSCF Profile is provisioned to activate PacketCable authentication, every UE that uses the affected P-CSCF profile is treated as a Packet Cable UE. Hence, it is recommended to add a P-CSCF Profile (in addition to the existing P-CSCF Profiles) as a dedicated Packet Cable P-CSCF profile.

## Before you begin

Observe the following:

- The P-CSCF must be available in the network.
- This procedure must be performed for every P-CSCF.

## Steps to activate Packet Cable authentication in P-CSCF profile

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **PCSCF Tables**.
- 2 In the left pane, expand the **PCSCF Profile** table group.
- 3 Double-click on the specific PCSCF table. Right-click on the desired entry and select **Modify Table Attributes**.  
**Result:** The **Pcscf Profile Attribute**stable populates.
- 4 Provision the following parameters in the **General Parameters** tab:

| Parameter                           | Provisioning   |
|-------------------------------------|--|
| <b>Remove P-Access-Network-Info</b> | Select the <b>Yes</b> option in the field to use the Packet Cable authorization scheme. This parameter removes the P-Access-Network-Info header from SIP messages. |

- 5 Provision the following parameters in the **Security Parameters** tab:

| Parameter                                   | Provisioning                               |
|---|--|
| IPSec Parameters group → Secure Server Port | This field must be kept blank or set to 0. |

- 6 Provision the following parameters in the **Miscellaneous Parameters** tab:

| Parameter                   | Provisioning                                    |
|-----------------------------|---|
| Support TISPAN e2 Interface | Select <b>Disabled</b> from the drop down list. |
| Access Type                 | Select <b>DOCSIS</b> from the drop down.        |

- 7 Click **OK**.

**Result:** The new values are updated.

END OF STEPS

# To provision SIP compression

## Purpose

This procedure is used to provision SIP compression for a P-CSCF profile.

## Before you begin

Observe the following:

- The P-CSCF must be available in the network.
- This procedure must be performed per P-CSCF and per SIPia port.

## Steps to provision SIP compression for P-CSCF profile

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → PCSCF Tables**.
- 2 In the left pane, expand the **PCSCF Profile** table group.
- 3 Double click on the specific PCSCF Table. Right-click on the desired entry and select **Modify Table Attributes**.

**Result:** The **Pcscf Profile Attributes** table populates.

| 4 | If you want to ...   | then ...  |
|---|----------------------|---|
|   | enable compression,  | <p>provision the following:</p> <ul style="list-style-type: none"> <li>• Select the <b>Compression Enabled</b> check box.<br/><i>Note:</i> The <b>Compression Enabled</b> check box only affects outgoing message compression. Incoming message decompression is always active (if needed) and is <i>not</i> affected by this check box.</li> <li>• Select the default compression technique from the <b>Default Compressor</b> menu.<br/><i>Note:</i> The <b>Default Compressor</b> selection only affects outgoing message compression. Incoming message decompression is always active (if needed) and is <i>not</i> affected by this selection.</li> <li>• Check the <b>Enforced Access</b> techniques to specify for which access techniques compression must be enforced.<br/><i>Note:</i> The <b>Enforced Access</b> selections, if any, are only used when screening incoming messages to ensure that they are in a compressed (SigComp) format. Outgoing message compression is <i>not</i> affected by the selections.</li> </ul> <p><i>End of procedure</i></p> |
|   | disable compression, | <p>Clear the <b>Compression Enabled</b> check box.</p> <p>The “Enforced Access” selections, if any, are only used when screening incoming messages to ensure they are in a compressed (SigComp) format. Outgoing message compression is <i>not</i> affected by the selections.</p> <p><i>End of procedure</i></p>   |

5 Click **OK**.

**Result:** The new values are updated.

END OF STEPS

# To provision IMS Signaling security

## Purpose

IMS signaling security is set up between the UE and the P-CSCF. All SIP signaling messages at the IP level are protected by IPSec. IPSec provides both confidentiality and integrity protection of SIP signaling between the UE and the P-CSCF. The authentication information is retrieved from the S-CSCF.

This procedure is used to provision IPSec settings on the P-CSCF and on the S-CSCF profile.

AKA is required for IMS signaling security using IPSec.

**Note:** The IPsec for ISC is only supported for cPSB in CP 4.1 and later. Access security with IPsec is supported only in configurations where Signaling firewall is enabled.

## Before you begin

The P-CSCF, S-CSCF must already be available in the network.

### Frequency

This procedure must be performed per P-CSCF, per S-CSCF and per IMS Server.

## 1. Security provisioning procedure in the P-CSCF profile

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → PCSCF Tables**.
- 2 In the left pane, expand the **PCSCF Profile** folder.
- 3 Double-click on the specific PCSCF table. Right click in an empty field of the table and select **Add Table Attributes** or **Modify Table Attributes** to add or modify a P-CSCF profile.

**Note:** If needed, the user can provision distinct data for integrity protection and confidentiality protection for SIP signaling between UE and P-CSCF.

- 4 Provision the following parameters in the **Security Parameters** tab.

| Parameter                             | Provisioning  |
|---------------------------------------|---|
| <b>Support IPsec Capable UEs Only</b> | Select this check box if the P-CSCF must only accept UEs that support IPSec access security.  |
| <b>SA Lifetime Shortened</b>          | Enter the value to define the shortened SA lifetime to allow NOTIFY to reach the UE during network initiated de-registration.   |
| <b>Secure Server Port</b>             | Enter the port number or retain the default value set to 0.   |
| <b>HMAC-MD5-96</b>                    | Define the priority of the IPSec integrity algorithm supported on the P-CSCF.   |
| <b>HMAC-SHA-1-96</b>                  | Define the priority of the IPSec integrity algorithm supported on the P-CSCF.   |
| <b>Support ESP Confidentiality</b>    | The P-CSCF does not perform encryption algorithm negotiation between the UE and P-CSCF, if this check box is <i>not</i> checked.  |
| <b>Require ESP Confidentiality</b>    | When <b>Support ESP Confidentiality</b> is performed and the check box is selected, the <b>Require ESP Confidentiality</b> check box appears. Select this check box if the P-CSCF does/does not require an encryption algorithm sent by the UE. |
| <b>DES-EDE3-CBC Priority</b>          | Select the correct encryption priority level for this encryption type.  |
| <b>Null Encryption Priority</b>       | Select the correct encryption priority level for this encryption type.  |
| <b>AES-CBC Priority</b>               | Select the correct encryption priority level for this encryption type.  |

- 5 Click **OK**.

**Result:** The new values are updated.

END OF STEPS

## 2. Security provisioning procedure in the S-CSCF profile

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → SCSCF Tables**.
- 2 In the left pane, expand the **SCSCF Profile** folder.

- 3 Double-click on the specific SCSCF table. Right-click the desired entry and select **Add Table Attributes** or **Modify Table Attributes** to add or modify an S-CSCF profile.

**Result:** The **SCSCF Profile Attributes** table populates.

- 4 Provision the following parameters in the **Authentication Options** tab:

| Parameter                       | Provisioning   |
|---------------------------------|--|
| Digest AKAv1 MD5                | Select the check box.  |
| Authenticate Protected Register | Select the check box.<br><b>Note:</b> This is an optional parameter. When this parameter is checked, a protected re-register/de-register request from UE still triggers an AKA authentication procedure. When the parameter is cleared, the S-CSCF responds with 200 OK. |

- 5 Click **OK**.

**Result:** The new values are updated.

END OF STEPS

# To provision the Service Based Local Policy Profile

## Purpose

This procedure is used to provision the Service Based Local Policy (SBLP) profile.

## Before you begin

**System requirements** - The P-CSCF must be available in the network.

## Procedure to add, rename, or delete the SBLP profile

Perform the following steps at the Provisioning GUI.

- 1 Navigate to **IMS > IMS General Tables**.

**Result:** The **IMS General Tables** window is displayed.

| 2 | If you want to...                                  | then...  |
|---|--|--|
|   | add a Service Based Local Policy Profile table,    | <ol style="list-style-type: none"><li>1. Right-click <b>Service Based Local Policy Profile</b>, and then select <b>Add Table</b>.</li><li>2. In the <b>Table Name</b> box, type a descriptive name and then click <b>OK</b>.</li></ol> <p><i>End of Steps.</i></p>   |
|   | rename a Service Based Local Policy Profile table, | <ol style="list-style-type: none"><li>1. Expand the <b>Service Based Local Policy Profile</b> folder.</li><li>2. Right-click the table that you want to rename, and then click <b>Rename Table</b>.</li><li>3. In the <b>Table Name</b> box, type a descriptive name and then click <b>OK</b>.</li></ol> <p><i>End of Steps.</i></p> |
|   | delete a Service Based Local Policy Profile table, | <ol style="list-style-type: none"><li>1. Expand the <b>Service Based Local Policy Profile</b> folder.</li><li>2. Right-click the table that you want to delete, and then click <b>Delete Table</b>.</li><li>3. Click <b>OK</b> to confirm deletion.</li></ol> <p><i>End of Steps.</i></p>  |

END OF STEPS

**Procedure to provision the SBLP table attributes**

Perform the following steps at the Provisioning GUI.

- 
- 1 Navigate to **IMS > IMS General Tables**.

**Result:** The **IMS General Tables** window is displayed.

- 
- 2 Expand the **Service Based Local Policy Profile** folder, and then double-click the Service Based Local Policy Profile table whose parameters you want to add, modify or delete.

**Result:** The right pane displays the Service Based Local Policy profiles that are currently defined. In the case of a newly created table this pane is initially empty.

---

| 3 | If you want to...                                     | then...  |
|---|---|--|
|   | add Service Based Local Policy Profile attributes,    | <ol style="list-style-type: none"> <li>1. On the menu bar, click <b>Attributes</b>, and then select <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SBLP Profile Attributes</b> window is displayed</li> <li>2. Proceed with <a href="#">Step 4</a>.<br/><i>End of Steps.</i></li> </ol>  |
|   | modify Service Based Local Policy Profile attributes, | <ol style="list-style-type: none"> <li>1. Select the profile that you want to modify.</li> <li>2. On the menu bar, click <b>Attributes</b>, and then select <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SBLP Profile Attributes</b> window is displayed</li> <li>3. Proceed with <a href="#">Step 4</a>.<br/><i>End of Steps.</i></li> </ol> |
|   | delete Service Based Local Policy Profile attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete.</li> <li>2. On the menu bar, click <b>Attributes</b>, and then select <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.<br/><i>End of Steps.</i></li> </ol>  |

- 
- 4 In the **General Parameters** tab, provision the following parameters:

- Profile ID
- Profile Description

- Diameter Interface Type
- AF Application Identifier

**Note:** The **AF Application Identifier** field identifies the service belonging to that session. This information is used by the PCRF to differentiate QoS for different application services.

- Audio Max Requested Uplink Bandwidth (kbps)
- Peak Bandwidth(kbps)
- Max Burst Size(kbits)
- Audio Max Requested Downlink Bandwidth (kbps)
- Peak Bandwidth(kbps)
- Max Burst Size(kbits)
- Video Max Requested Uplink Bandwidth (kbps)
- Peak Bandwidth(kbps)
- Max Burst Size(kbits)
- Video Max Requested Downlink Bandwidth (kbps)
- Peak Bandwidth(kbps)
- Max Burst Size(kbits)
- Message Max Requested Uplink Bandwidth (kbps)
- Peak Bandwidth(kbps)
- Max Burst Size(kbits)
- Message Max Requested Downlink Bandwidth (kbps)
- Peak Bandwidth(kbps)
- Max Burst Size(kbits)
- Other Max Requested Uplink Bandwidth (kbps)
- Peak Bandwidth(kbps)
- Max Burst Size(kbits)
- Other Max Requested Downlink Bandwidth (kbps)
- Peak Bandwidth(kbps)
- Max Burst Size(kbits)
- Reserve Bandwidth per SDP Local Policy

**Note :** This check box is used for bandwidth reservation when B=AS line is not present in the SDP. When this check box is selected it allows the AF(P-CSCF) to use configured bandwidth per media sub-type(for example per audio/video codec or by MSRP media type) in SDP local policy for resource reservation. When this check box is not selected, then the AF uses the configured max requested bandwidth per media type in the SBLP profile.

- Enhanced Data Rate Control per Local Policy

**Note:** If this check box is selected then the AF (P-CSCF) is allowed to use additional H.248.53 (tman) traffic management parameters for enhanced traffic policing per media type. When this check box is cleared, then the AF(P-CSCF) uses the configured default tman parameters specified in the SBLP profile.

- External Ingress Uplink Early Media Enabled
- External Ingress Downlink Early Media Enabled
- External Egress Uplink Early Media Enabled
- External Egress Downlink Early Media Enabled
- Close Gates Due to SIP Forking

**Note:** By default, this check box is selected.

- Keep Session on Zero Packet
- IPv6 Unspecified Address Format

In the **TISPA Parameters** tab, configure the following parameters:

- Policy Server FQDN
- Near End NAPT Control
- Detect Far End NAPT
- Border Gateway Bypass
- Bypass Invoking the BGF for MSRP Traffic

**Note:** The **Bypass Invoking the BGF for MSRP Traffic** flag was added in SBLP profile to turn off MSRP support. If the **Bypass Invoking the BGF for MSRP Traffic** check-box is selected, the MSRP traffic does not perform the NAPT. (This flag was added because 7510 does not support TCP traffic).

- Authorization Lifetime (seconds)
- Authorization Refresh (seconds)
- Media Negotiation Support
- Remove GW When Media Agnostic Mode
- Primary Policy Server Destination FQDN
- Alternative Policy Server Destination FQDN
- Modify Setup In SDP Answer

In the **3GPP Parameters** tab, configure the following parameters:

- 3GPP TS 29.214 Rx Version

**Note :** The **3GPP TS 29.214 Rx Version** field defines the version supported by 3GPP TS 29.214 for the Rx interface. The field **3GPP TS 29.214 Rx Version** can be set to one of the following values:

- **R8 v8.4.0** - the Supported-Features AVP is mandatory and the message is rejected when the AVP is not present.
- **R8 v8.7.0** - the Supported-Features AVP is mandatory only in the initial AAR/AAA message.
- **R9 v9.4.1** - the Supported-Features AVP is mandatory only in the initial AAR/AAA message.
- **R10 v10.4.0** - the Supported-Features AVP is mandatory only in the initial AAR/AAA message.
- Reject SIP Request when BGW Realm unavailable

This flag can only be set to ‘Yes’ when the global flag “Relay Realm Status to AF” is set to ‘Yes’.

- Primary Policy Server Destination FQDN
- Alternative Policy Server Destination FQDN
- Subscription to Notification of Signaling Path Status
- Provision AF Signalling Flow

This flag is available only when the flag **3GPP TS 29.214 Rx Version** is set to **R9 v9.4.1** or beyond.

This flag is applicable to the interface type **3GPP** and **TISPAN/3GPP**.

---

5 Click **OK**.

**Result:** The SBLP attributes are provisioned successfully.

For more information on the SBLP parameters, see “**Service Based Local Policy Profile**” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specifications and Object Descriptions Manual*, 275-900-379 .

END OF STEPS

---

# To provision e2 interface support

## Purpose

This topic describes the task flow to provision support for the TISPAN e2 interface.

The e2 interface is the interface between the P-CSCF and the CLF as defined in TISPAN NASS specifications.

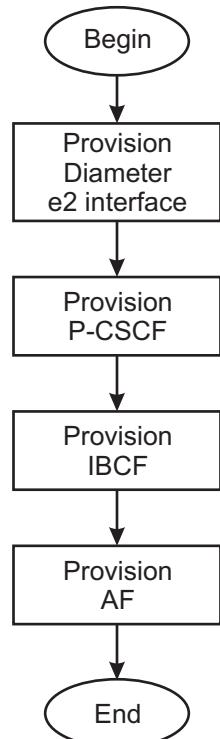
## CLF provisioning

Configuration of the CLF that is connected through the e2 interfaces is out of the scope of this document. CLF configuration depends on the network element that provides the CLF functionality.

See also, the documentation of the CLF network element.

## Task flow

e2 interface provisioning task flow:



## Task flow stages

- 
- Configure a Diameter application ID for the e2 interface.

Configure the following parameters:

| Parameter | Value              |
|-----------|--------------------|
| e2        | Default = 16777231 |

**Reference:** “To modify Diameter application IDs” (p. 10-31).

---

- Configure a Diameter profile that supports the e2 interface as a Diameter Connection Interface.

Configure the following parameters:

| Parameter                | Value                                |
|--------------------------|--------------------------------------|
| Application Type         | e2                                   |
| Destination FQDNType     | Enter the FQDN of the CLF.           |
| Alt Destination FQDNType | Enter the FQDN of the alternate CLF. |

Use the default values for the other parameters.

**Reference:** “To provision a Diameter profile” (p. 10-23).

---

- Verify that a service to Diameter mapping exists for the Service Type IMS. The Diameter profile that is assigned to the Service Type must include the e2 interface.

**Reference:** “To provision a Service to Diameter mapping” (p. 10-32).

---

- Configure the P-CSCF profile for e2 interface support.

Configure the following parameters:

| Parameter   | Value  |
|---|--|
| <b>Support TISPAN e2 Interface</b>                | <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Use-IP</b></li> <li>• <b>Use-PUID</b></li> <li>• <b>Use-PRID</b></li> </ul> <p>This option is used to specify whether the TISPAN e2 interface is enabled or disabled on the P-CSCF. Based on the selected option (Use-IP , Use-PUID, or Use-PRID), the P-CSCF uses the UE IP address, the Public User ID, or the private ID in e2 query.</p> <p><b>Note:</b> The following parameters: <b>Application Function Identifier</b>, <b>Access Type</b> and <b>Published Realm</b> that is located in the General Parameters tab must be provisioned</p> |
| <b>Application Function Identifier</b>            | <p>Enter an identifier. The identifier is used by the CLF to validate the P-CSCF.</p> <p>This option is applicable when the TISPAN e2 Interface option is enabled.</p>   |
| <b>Default PANI for e2 interface for REGISTER</b> | <p>Enter a PANI value for the REGISTER message.</p> <p>This field specifies the PANI value that the P-CSCF should insert as the value for the PANI header when failure occurs in the CLF query through the e2 interface for the REGISTER message.</p> <p>This option is applicable when the TISPAN e2 Interface option is enabled.</p>   |
| <b>Default PANI for e2 interface for INVITE</b>   | <p>Enter a PANI value for the INVITE message.</p> <p>This field specifies the PANI value that the P-CSCF should insert as the value for the PANI header when failure occurs in the CLF query through the e2 interface for the INVITE message.</p> <p>This option is applicable when TISPAN e2 Interface option is enabled.</p>   |

| Parameter                    | Value  |
|------------------------------|--|
| Access Type                  | Select a value to reflect the type of access network that is supported by the P-CSCF.<br><br>Examples of an access network type: <ul style="list-style-type: none"> <li>• ADSL</li> <li>• HDSL</li> <li>• IEEE-802.11</li> </ul> |
| IP Address Realm             | Enter a valid realm that allows the CLF to distinguish this realm from other realms the CLF interfaces with.   |
| Remove P-Access-Network-Info | Select <b>Yes</b>  |

**Reference:** “To provision PCSCF profile” (p. 4-77).

- 5 If an IBCF is used in the network, and one of the P-CSCFs in the network uses the e2 interface, configure the IBCF profile to remove P-headers.

Configure the following parameters:

| Parameter                    | Value |
|------------------------------|-------|
| Remove P-Access-Network-Info | Yes   |

**Reference:** “To provision IBCF Profile” (p. 4-198).

- 6 Provision the applications that use information that is retrieved from the CLF information using the e2 interface.

The following applications are examples of applications that use CLF information:

- NASS-bundled authentication (provisioned through the S-CSCF profile)
- Emergency services (provisioned through the P-CSCF profile)

# Support to provide P-CSCF IP address to UE

## Overview

The “Support to provide P-CSCF IP address to UE” feature provides an option for the P-CSCF to specify its IP address and port number in the SIP headers sent to the UE, instead of providing the usual P-CSCF FQDN. This feature can be enabled in case devices in the access network are not able to perform DNS queries on the P-CSCF FQDN.

The **Provide P-CSCF IP Address to UE** check box in the P-CSCF profile should be selected to include the IP address and port number in the SIP headers. To enable the functioning of the feature, ensure that the **Enable Two NIs for SIP** check box is selected in the SIPia port assigned to the P-CSCF profile, as the external network interface provides the IP address and port number to the UE.

The SIP message headers which include the IP addresses are as follows:

- Contact header for the messages exchanged during an INVITE dialog: that is, INVITE request, 1xx or 2xx response to INVITE, and messages sent within INVITE dialog (for example, re-INVITE, UPDATE, OPTIONS and MESSAGE)
- Record-Route header for the messages exchanged during a SUBSCRIBE/REFER dialog: that is, SUBSCRIBE/REFER request, 1xx or 2xx response to SUBSCRIBE/REFER, and messages sent within SUBSCRIBE/REFER dialog (for example, NOTIFY request and re-SUBSCRIBE request)
- Service-Route header for the 200 OK response to the REGISTER request

When the P-CSCF is dual-stack and provisioned with both IPv4 and IPv6 addresses, the P-CSCF sends an IP address that matches the type of address assigned to the UE. The IP format of the UE is derived from the Contact and Via header.

**Note:** This feature is available only on 5400 LCP.

# To provision the TLS Profile table

## Purpose

This procedure is used to provision the TLS profile table.

## Steps to provision the TLS Profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS General Tables → TLS Profile**.
- 2 Expand the **TLS Profile** table group. Double-click on the specific TLS table.
- 3 

| If you want to ...               | then ...   |
|----------------------------------|--|
| add a TLS Profile table,         | select <b>Attributes → Add Table Attributes</b> . Only one table can be added.<br><b>Result:</b> The <b>TLS Profile Attributes</b> window is displayed.  |
| rename a TLS Profile table name, | select the table you want to rename, and select <b>Rename Table</b> from the Tables menu.<br>Rename the table and click <b>OK</b> .  |
| delete a TLS Profile table,      | select the table you want to delete, and select <b>Tables → Delete Table</b> from the menu.<br>Click <b>OK</b> .<br><b>Note:</b> The TLS profile cannot be deleted, if it is referred to a Service-Based PCSCF profile of a P-CSCF with a TLS server port set. |
- 4 Right-click in an empty field and select **Add Table Attributes** or **Mofidy Table Attributes** to add or modify table attributes for a TLS Profile. Configure the following parameters in the **TLS Profile Attributes** window:

| Parameter             | Provisioning                             |
|-----------------------|--|
| <b>TLS Profile ID</b> | Select the TLS Profile ID from the list. |
| <b>Description</b>    | Enter the TLS Profile description.       |

| Parameter                                      | Provisioning   |
|--|--|
| <b>Certificate Verification Depth</b>          | Certificate verification depth is used to control the searching depth. The valid range of verification depth is from 1 to 12. The default value is 4.  |
| <b>Enable Mutual Authentication (Gm only)</b>  | This field is disabled by default.   |
| <b>Ciphersuites-encryption Algorithms List</b> | <p>Add at least one Ciphersuites-encryption Algorithm.</p> <p>To add an algorithm,</p> <ol style="list-style-type: none"> <li>1. Select the algorithm from the list on the left pane.</li> <li>2. Click <b>Add -&gt;</b>. The selected algorithm moves to the list box on the right.</li> </ol> <p>To remove an algorithm from the selected list,</p> <ol style="list-style-type: none"> <li>1. Select the algorithm from the list box on the right.</li> <li>2. Click <b>&lt;- Delete</b>. The selected algorithm is removed from selection.</li> </ol> |
| <b>Ciphersuites-hash Algorithms List</b>       | <p>Add at least one Ciphersuites-hash Algorithm.</p> <p>To add an algorithm</p> <ol style="list-style-type: none"> <li>1. Select the algorithm from the list on the left pane.</li> <li>2. Click <b>Add -&gt;</b>. The selected algorithm moves to the list box on the right.</li> </ol> <p>To remove an algorithm from the selected list,</p> <ol style="list-style-type: none"> <li>1. Select the algorithm from the list box on the right.</li> <li>2. Click <b>&lt;- Delete</b>. The selected algorithm is removed from selection.</li> </ol>        |

5 Click OK.

END OF STEPS

# To provision the SIP Error Treatment Table attributes

## Purpose

This procedure is used to provision the SIP Error Treatment Table attributes.

## Procedure

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS > IMS General Tables > SIP Error Treatment Table**.
- 

- 2 Expand the **SIP Error Treatment Table** table group.
- 

| 3 | If you want to ...                  | then ...  |
|---|-------------------------------------|---|
|   | add a SIP Error Treatment table,    | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table Attributes</b>.<br/><b>Result:</b> The <b>Add SIP Error Treatment Table</b> window appears. The user can add only one table.</li><li>2. Select the <b>Table number</b> from the list.</li><li>3. Enter <b>Table name</b> and click <b>OK</b>.</li></ol> |
|   | rename a SIP Error Treatment table, | <p>select the table you want to rename, and select <b>Tables &gt; Rename Table</b>.<br/>Rename the table and click <b>OK</b>.</p>   |
|   | delete a SIP Error Treatment table, | <p>select the table you want to delete, and select <b>Tables &gt; Delete Table</b>.<br/>Click <b>OK</b>.</p>  |

- 
- 4 Click on the table, and select **Add Table Attributes** or **Modify Table Attributes** to add or modify table attributes. Similarly the **Delete Table Attributes** can be selected to delete table attributes.

**Result:** The **SIP Error Treatment Table Attributes** window is displayed.

---

- 5 Provision the following parameters:

| Parameter | Provisioning                                 |
|-----------|--|
| Record ID | Select the record ID from the drop down box. |

| Parameter             | Provisioning  |
|-----------------------|---|
| <b>Category</b>       | Select the SIP error code category from the drop down box.<br>The available options are: <ul style="list-style-type: none"><li>• Cx</li><li>• Routing</li><li>• Authentication</li><li>• ENUM Query</li></ul>   |
| <b>Internal Code</b>  | Select the internal error code. The options are listed in the table below.  |
| <b>SIP Error Code</b> | Select the SIP Error code from the list. The value ranges from 400 to 699.  |
| <b>Text</b>           | Enter the text to be included in warning text, reason text, or reason phrase (top line of the SIP error response), depending on the value of text usage. The value “NULL” means no Warning header or Reason header needs to be included.  |
| <b>Text Usage</b>     | Select one of the options from the drop down box to specify the location to include the descriptive text as defined in text field.<br>The available options are as follows: <ul style="list-style-type: none"><li>• Reason Header</li><li>• Warning Header</li><li>• Reason Phrase</li><li>• XML Body</li></ul> |

The options for the **Internal Code** varies based on the selected Category and are listed below:

| Cx                         | Routing               | Authentication              | ENUM Query                      |
|----------------------------|-----------------------|-----------------------------|---------------------------------|
| UAA_User_Unknown,          | REG_Routing_Failure   | Challenge_Response_Mismatch | ENUM Failure                    |
| UAA_Roaming_Not_Allowed    | PCSCF_Routing_Failure |                             | No CgPN for ENUM Query Found    |
| UAA_Authorization_Rejected |                       |                             | ENUM Query Disallowed           |
| LIR_Failure                |                       |                             | R-URI ineligible for ENUM Query |

| Cx                                       | Routing | Authentication | ENUM Query                |
|--|---------|----------------|---------------------------|
| LIA_Identity_Not_Registered              |         |                | ENUM returned<br>Void     |
| SAA_Diameter_Identity_Already_Registered |         |                | ENUM returned<br>NXDOMAIN |

- 6 Click **OK**.

END OF STEPS

---

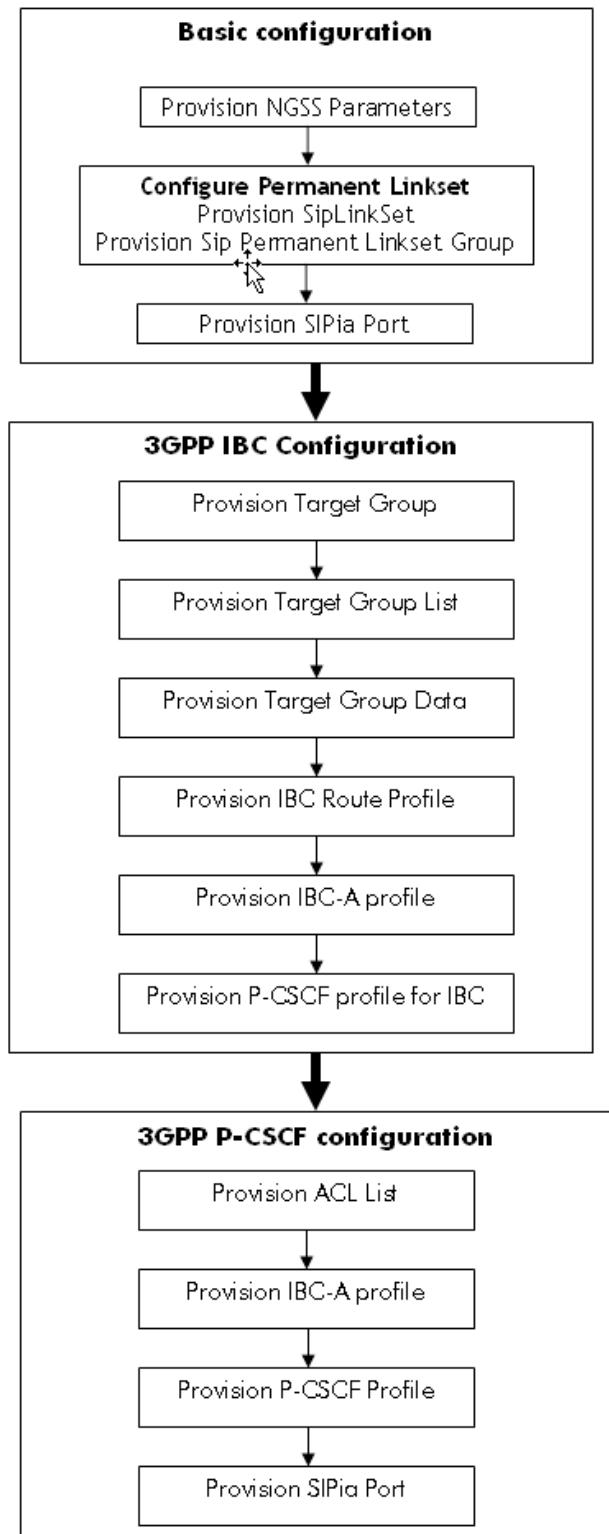
## Provisioning Task flow - To provision P-CSCF pool

### Purpose

This provisioning task flow provides the steps to provision P-CSCF pool.

## Provisioning task flow diagram

The following figure illustrates the provisioning task flow for provisioning the P-CSCF pool.



## Basic configuration task flow

Perform the following steps to enable P-CSCF pool mode:

**1** Provision NGSS Parameters.

Provision the following parameters:

- Enable **SIP Session Parameters** group
- Enable **Send 100 Trying in response to non-INVITE request**
- Enable **Immediately send 100 Trying in response to MESSAGE**
- Enable **P-CSCF Pool Mode**
- **P-CSCF Pool Domain:** Type the P-CSCF pool domain string

See “[To provision NGSS Server parameters](#)” (p. 10-9).

**2** To setup heartbeat from S-CSCF to P-CSCF, do the Permanent LinkSet configuration

Provision an SIP LinkSet as follows:

- Enable **DNS**
- **Destination FQDN:** Type the P-CSCF FQDN (for example, *pcsf-stdn.imsgroup0-000.gll12.ate.lucentlab.com*)

See “[To provision an SIP Linkset](#)” (p. 4-264).

**3** Provision an SIP Permanent LinkSet Group.

**Linkset ID:** Select a LinkSet

See “[To provision an SIP Permanent Linkset Group](#)” (p. 4-269).

**4** Provision the SIPia Port.

**Sip Permanent Linkset Group Number:** Select the Linkset Group provisioned for SCSCF SIPia port

See “[To provision a SIPia port](#)” (p. 10-40).

## 3GPP IBC configuration

**1** Provision a Target Group.

Provision the following parameters:

- Set **Location** as “Core”
- Set **Target Type** as “Domain”
- Set **Target Host Name** as FQDN (not IPs) for PCSCF pool, and the configuration must match with the data in DNS
- Enable **Enable Heartbeat**

See “[To provision Target Group Table](#)” (p. 5-304)

---

## 2 Provision a Target Group List

Create a target group list with existing target groups. The target group data is provisioned based on the existing target groups.

See “[To provision Target Group Table](#)” (p. 5-304)

---

## 3 Provision an IBC Route Profile

**Default Proxy:** Select the target group

See “[To provision IBC Route Profile](#)” (p. 5-297)

---

## 4 Provision the following IBC-A Profile parameters:

- Set **Apply Privacy** as Yes (recommended value)
- Set **Provide P-CSCF IP Address to Core** as No (recommended value)
- Set **Support 3xx** as No (recommended value)
- Set **Disable 3GPP Headers** as No (recommended value)
- Set **Contact Rewrite** as Yes (recommended value)
- Set **Path header not included** as Yes (recommended value)
- Set **Don't Subscribe to 'reg' Event** as Yes (recommended value)
- Set **Service-Route not required** as No (recommended value)
- Set **P-Associated-URI not required** as No (recommended value)
- Set **Use Derived Private-ID** as No (recommended value)
- Set **Use Registry Cache Data** as Yes (recommended value)
- Set **Allow Unregistered Calls** as Emergency Only (recommended value)
- Set **Insert ue-addr** as Yes (recommended value)

See “[To provision IBC-A Profile](#)” (p. 5-290)

---

## 5 Provision a PCSCF profile for IBC

---

Provision the PCSCF Profile → General Parameters

- Enable **Provide P-CSCF IP Address to UE**
- Enable **Encode Contact Data**
- Enable **Activate SIP Header Reduction**
- Enable **UDP Symmetric Response Routing**
- Enable **End-to-End Treatment for BYE**
- Enable **SIP Topology Hiding**
- Set **IBC-Access Mode** as “3GPP IBC”
- **IBC-A Profile ID:** set the IBC-A Profile
- **Published Realm:** set the published realm
- Enable **Registration Suppression only when NAT detected**
- Enable **Apply Registration Suppression only when NAT detected**

See “[To provision PCSCF profile](#)” (p. 4-77)

---

**6** Provision the PCSCF Profile → Security Parameters

Enable **Enable IP Association** for 3GPP IBC

From the **IP Association Source Granularity** drop-down list, select “IP Address and Port ”.

See “[To provision PCSCF profile](#)” (p. 4-77)

---

**7** Provision the P-CSCF Profile → Miscellaneous Parameters

Provision the following parameters

- Enable **SBLP Enabled**
- **SBLP Profile ID:** Set the SBLP profile

See “[To provision PCSCF profile](#)” (p. 4-77)

## 3GPP PCSCF Configuration

---

**1** Provision the ACL List

Provision the following parameters that are allowed for unregistration origination requests:

- Start IP Address
- End IP Address

- Lower Port
- Upper Port

See “[To provision ACL List](#)” (p. 5-322)

- 
- 2 Add a new Profile ID for IBC-A Profile and provision the parameters as follows:
- Set **Allow Unregistered Originations** as ACL List Only
  - From the **Permanently Trusted Non-Registering Users List** drop-down list, select the ACL List table ID
  - The other parameters must be disabled.
- See “[To provision IBC-A Profile](#)” (p. 5-290)
- 
- 3 In the PCSCF profile of 3GPP PCSCF, associate the IBC-A Profile ID with ACL List table. Provision the P-CSCF Profile as follows:
- On the General Parameters tab, set the **IBC-A Profile ID**
  - On the Security Parameters tab, provision as follows:
    - Disable **Enforce Initial Request**
    - Set **Security Gateway Profile Id** as None
    - Disable **Enable IP Association**
  - For PCSCF profile of 3GPP PCSCF, and if the PCSCF is working with 3GPP IBC, disable the distributed IP, 2 NIs, FEPH, IP association, and iSGW.
- See “[To provision PCSCF profile](#)” (p. 4-77).
- 
- 4 In the Service-Based PCSCF profile, enable **Heartbeat SCSCF**.
- See “[To provision Service-Based PCSCF Profile](#)” (p. 4-69).
- 
- 5 In the SIPia Port Configuration window, disable **Enable Two NIs for SIP**.
- See “[To provision a SIPia port](#)” (p. 10-40).

# BGCF provisioning

## Overview

### Purpose

This section provides the procedures that are used to provision the Breakout Gateway Control Function (BGCF).

### Contents

|  |       |
|--|-------|
| To provision BGCF URI Id                                     | 4-133 |
| To provision BGCF Target List                                | 4-138 |
| To provision BGCF Profile                                    | 4-142 |
| To provision BGCF Time Of Day                                | 4-148 |
| To provision BGCF Network Gateway                            | 4-152 |
| To provision BGCF Default Network Gateway                    | 4-156 |
| To provision Originating Host Class Profile routing for BGCF | 4-160 |
| To provision Subscriber Profile routing for BGCF             | 4-163 |
| To provision BGCF DA Route Table                             | 4-172 |
| To provision BGCF SIP content type                           | 4-177 |
| To provision BGCF local number routing                       | 4-181 |
| To provision BGCF location based routing                     | 4-189 |
| To provision BGCF Originating Host ID                        | 4-193 |

# To provision BGCF URI Id

## Purpose

This procedure is used to provision a BGCF URI Id table.

Target URI is the individual SIP destination that the BGCF can send a request to. It is sometimes referred to as next hop of destination. Heartbeat and SDP media capability should be associated with each Target URI.

## When you *add* a BGCF URI Id table

When you *add* a new BGCF URI Id table, it is empty. You must still add BGCF URI Id attribute.

## Before you *delete* a BGCF URI Id table

Before you *delete* a BGCF URI Id table, you must make sure that there are no BGCF URI Ids that are used by the BGCF Route Table.

## About IPv6 addresses

If the Target URI type is IPv6, the following conditions must be true:

- The address must be enclosed in [ ].
- An optional port number may be included in the URI, it is separated by a ":" immediately following the [ ].
- IPv6 address checks within the [ ], the condensed IPv6 address form is supported.
- Two to seven ":" are allowed.
- Zero to four hexadecimal digits are allowed between two ":".
- "::" may appear at most once in the field.
- IPv4 can only appear at the last 32 bits of the address.

### Examples of IPv6:

Target URI: **[2001:db8::9:01]**

**[2001:db8::10]:5070**

## Before you begin

Observe the following:

### Frequency

This procedure must be carried out whenever a BGCF URI Id table must be provisioned.

### Required information

This procedure is performed at the Provisioning GUI.

## Steps to provision a BGCF URI Id table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **BGCF Tables**.

**Result:** The **BGCF Tables** window is displayed.

- 2 In the left pane, expand the **BGCF URI Id** folder.

**Result:** The BGCF URI Id tables are listed under the folder in the left pane.

If the folder is empty, add a BGCF URI Id table.

Perform the following steps in the **BGCF Tables** window to add, rename, or delete a BGCF URI Id table :

| If you want to ...          | then ...  |
|-----------------------------|---|
| add a BGCF URI Id table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a BGCF URI Id table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |
| delete a BGCF URI Id table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a BGCF URI Id table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>  |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the BGCF URI Id table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **BGCF Tables** window to add, modify, or delete the BGCF URI Id table attributes:

| If you want to ...                     | then ...  |
|--|---|
| add the BGCF URI Id table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol>   |
| modify a BGCF URI Id table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol> |
| delete a BGCF URI Id table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.<br/><i>End of steps.</i></li> </ol>               |

**5** Provision the following parameters:

| Parameter              | Provisioning   |
|------------------------|--|
| <b>Target URI ID</b>   | Select target URI id in <b>Target URI ID</b> that should be mapped to a URI.   |
| <b>Target URI</b>      | <p>Enter the URI of the target MGCF or BGCF in the <b>Target URI</b> field (the IMS node which should further route the INVITE message to the PSTN).</p> <p>Note that the default port number that is used for sending the SIP messages is IP port 5060. If another port number is desired you can specify this by adding a ":" followed by the <b>"port number"</b>.</p> <p><b>P-NAPTR configuration</b></p> <p>No P-NAPTR lookup is done for the BGCF URI table , therefore the <b>Target URI</b> should include the Generic URI Label (GUL) and local domain zone (bgcf-stdn.east.example.com).</p> |
| <b>Target URI Type</b> | Select the target URI type from the <b>Target URI Type</b> field. The available options are <b>Domain</b> , <b>IPv4</b> , <b>IPv6</b> and <b>Text string</b> .   |
| <b>Heartbeat</b>       | If desired select the <b>Heartbeat</b> parameter. BGCF sends heartbeat messages to the target destination to determine if the link is active. In case the link is down, an alarm is generated via the MI GUI. Calls to this target are blocked and BGCF attempts other provisioned routes. When the heartbeat option is not selected, calls are processed as normal with no status check   |
| <b>Admin State</b>     | If desired lock or unlock the <b>Admin State</b> . Selecting <b>Lock</b> renders the URI unusable for routing calls. Heartbeat is allowed, but no call traffic is allowed.   |
| <b>Digit Table Id</b>  | Select the appropriate value for the digit table from the <b>Digit Table Id</b> drop-down list.  |

| Parameter              | Provisioning  |
|------------------------|---|
| <b>SDP Media Types</b> | <p>Select the SDP media type(s) associated with the target URI in the <b>SDP Media Types</b> section:</p> <ul style="list-style-type: none"> <li>• Audio</li> <li>• Video</li> <li>• Application</li> <li>• Data</li> <li>• Control</li> <li>• Text</li> <li>• Message</li> </ul> <p><b>Routing based on SDP type</b></p> <p>BGCF supports routing based on incoming SDP media type in the INVITE message. After getting the Target URIs, and before routing the call, the parameter <b>Routing based on SDP media type</b> is checked. If this parameter is set to "Yes", the routing based on SDP media type is applied. The target URIs are checked to match with incoming SDP media types. The priority of URIs is determined first by media type match, then the Q-priority if there are equal matches of the media types. If there are "N" number of "m=" lines in the incoming SDP, the target URIs are screened in the incoming "m=" line sequence for each media type, the URIs that can support all of the incoming media types are selected.</p> |

For more information on the parameters, see the topic **Add Target URI** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

**6** Click **OK**.

**Result:** The BGCF URI Id table attributes are provisioned successfully.

END OF STEPS

# To provision BGCF Target List

## Purpose

This procedure is used to provision a BGCF Target List table.

A Target URI list is a group of URIs which are selected from the Target URIs that are associated with the destination for a specific digit analysis routing table entry. Any of the URIs in the list is able to reach a destination based on the digit analysis. In the list, each URI has a q value associated with it. One of the URI in the Target list is chosen for routing. Usually, the selected URI has the highest q value. It can also be the URI that has the best matched media type.

## When you *add* a BGCF Target List table

When you *add* a new BGCF Target List table, it is empty. You must still add BGCF Target List attribute.

## Before you *delete* a BGCF Target List table

Before you *delete* a BGCF Target List table, ensure that no BGCF Target List are used by the BGCF Digit analysis.

## Before you begin

Observe the following:

### Frequency

This procedure must be performed whenever a BGCF Target List table must be provisioned.

### Required information

This procedure is performed at the Provisioning GUI.

## Steps to provision a BGCF Target List table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS** → **IMS Components** → **BGCF Tables**.

**Result:** The **BGCF Tables** window is displayed.

- 
- 2 In the left pane, expand the **BGCF Target List** folder.

**Result:** The BGCF Target List tables are listed under the folder in the left pane.

If the folder is empty, add a BGCF Target List table.

Perform the following steps in the **BGCF Tables** window to add, rename, or delete a BGCF Target List table:

| If you want to ...               | then ...  |
|----------------------------------|---|
| add a BGCF Target List table,    | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a BGCF Target List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a BGCF Target List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a BGCF Target List table, ensure that no table entries are in use.</p> <p><i>End of steps</i></p>  |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the BGCF Target List table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **BGCF Tables** window to add, modify, or delete the BGCF Target List table attributes:

| If you want to ...                          | then ...  |
|---|---|
| add the BGCF Target List table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a BGCF Target List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a BGCF Target List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>           |

- 5 Provision the following parameters:

| Parameter | Provisioning                  |
|-----------|-------------------------------|
|           | Add a <b>Target List ID</b> . |

| Parameter | Provisioning  |
|-----------|---|
|           | <p>Enter the description of the Target URI in the <b>Description</b>.</p> <p>Click <b>Add</b> to add a URI from the list of provisioned Target URIs and assign an appropriate Q-value to the Target URI.</p> <p>Click <b>OK</b>.</p> <p>Add additional Target URIs and Q-values as needed.</p> <p><b>Note:</b> Traffic to Target URIs of equal Q-value is evenly distributed.</p> |

For more information on the parameters, see the topic **Add Target URIQPriority List** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

**6** Click **OK**.

**Result:** The BGCF Target List table attributes are provisioned successfully.

END OF STEPS

# To provision BGCF Profile

## Purpose

This procedure is used to provision a BGCF Profile.

## Before you begin

Observe that the following information is provisioned prior to the beginning of this procedure:

- BGCF URI Id
- BGCF Target List
- BGCF Digit Analysis (DA) Route table.
- BGCF Originating Source Info table.
- BGCF Local Number Routing table.

Depending on routing needs, other tables may need to be provisioned.

BGCF SIPia Port must be provisioned after the BGCF Profile.

## Steps to provision a BGCF Profile table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS** → **IMS Components** → **BGCF Tables**.

**Result:** The **BGCF Tables** window is displayed.

---

- 2 In the left pane, expand the **BGCF Profile** folder.

**Result:** The BGCF Profile tables are listed under the folder in the left pane.

If the folder is empty, add a BGCF Profile table.

Perform the following steps in the **BGCF Tables** window to add, rename, or delete a BGCF Profile table :

| If you want to ...           | then ...  |
|------------------------------|---|
| add a BGCF Profile table,    | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a BGCF Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a BGCF Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a BGCF Profile table, you must make sure that the profile is NOT used by an SIPia port.</p> <p><i>End of steps.</i></p>                          |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the BGCF Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **BGCF Tables** window to add, modify, or delete the BGCF Profile table attributes:

| If you want to ...                      | then ...  |
|---|---|
| add the BGCF Profile table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a BGCF Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a BGCF Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>           |

- 5 Provision the following parameters:

| Parameter                  | Provisioning  |
|----------------------------|---|
| <b>Profile Description</b> | Enter the description of the BGCF Profile in the <b>Profile Description</b> . |
| <b>DA Route Table ID</b>   | Select the digit analysis table defined in the <b>DA Route Table ID</b> .     |

| Parameter   | Provisioning  |
|---|---|
| Originating Source Info Table ID  | Select the Originating Source Info Table ID defined in the <b>Originating Source Info Table ID</b> list.  |
| Default Local Number Routing Table ID   | Select the Default Local Number Routing Table ID defined in the <b>Default Local Number Routing Table ID</b> list.  |
| ACR Charging Profile ID   | Select the ACR Charging Profile ID to which the BGCF needs to be mapped in the <b>ACR Charging Profile ID</b> list.<br><br><b>Note:</b> ACR Charging Profile with ID 0 is regarded as a default profile. The default profile is mapped to 3GPP version 5 ACR messages. The content of default profile is not changeable through the FS GUI. If the BGCF is correlated to default profile and you need to change the version, you can add a new ACR charging profile with the expected version selection and associate the BGCF to the new ACR charging profile. |
| ACR Charging Profile ID   | Select the ACR Charging Profile ID in the <b>ACR Charging Profile ID</b> list.  |
| Routing Precendence   | Select the routing precedence from the <b>Routing Precendence</b> list. When both CIC and RN are received in the incoming call, this setting determines which parameter to process.   |
| Remove Network Private Headers<br>[P-Charging Vector and P-Access-Network-Info] | Enable <b>Remove Network Private Headers [P-Charging Vector and P-Access-Network-Info]</b> if you want to remove the Network Private Headers from the outgoing messages.<br><br><b>Note:</b> The Network Private Headers are removed from the outgoing messages if the requests are sent outside of the IMS network, irrespective of whether the parameter <b>Remove Network Private Headers [P-Charging Vector and P-Access-Network-Info]</b> is enabled or disabled.  |
| SIP Proxy Mode  | Enable <b>SIP Proxy Mode</b> if you want the BGCF to act as SIP proxy.  |

| Parameter  | Provisioning  |
|--|---|
| <b>Process Redirect Outside of Home Domain</b>         | Enable the <b>Process Redirect Outside of Home Domain</b> check box to set the redirect address home domain when a redirect message is received by BGCF.  |
| <b>Use CgPN in P-Served-User and Diversion Headers</b> | Enable the <b>Use CgPN in P-Served-User and Diversion Headers</b> check box for the BGCF to use P-Served-User and Diversion headers as the CgPN for routing, if either of the headers is included in the request. |
| <b>Routing Based on Originating Host Identifier</b>    | Select the <b>Enable</b> check box if you want to enable the service, and then provision the next parameter, else Click <b>OK</b> and exit.   |
| <b>Originating Host Identifier For Routing</b>         | Select either <b>Calling Party Identity</b> or <b>X-LU-Orig-Host header</b> in the <b>Originating Host Identifier For Routing</b> combo box, to identify the source for retrieving the originating host.          |
| <b>Default Handling Option</b>                         | Select the appropriate action in the <b>Default Handling Option</b> combo box to define the action in case no match is found for the originating host.  |
| <b>Default Location Based Routing Table</b>            | Select the relevant table ID from the <b>Default Location Based Routing Table</b> combo box.  |
| <b>Digit Analysis</b>                                  | In the <b>Digit Analysis</b> section, select the appropriate value of the digit table from the <b>Digit Table Id</b> drop-down list.  |
| <b>Perform Digit Analysis in Proxy Mode</b>            | Enable the <b>Perform Digit Analysis in Proxy Mode</b> check box to select the digit manipulation in the proxy mode.  |
| <b>Forward request by Adding Route Header</b>          | Enable the <b>Forward request by Adding Route Header</b> check box to route calls with the next hop in the Route header instead of the R-URI.   |
| <b>CRF Route Profile ID</b>                            | None – IDs of the CRF Route Profiles  |
| <b>SIP Error Treatment Table ID</b>                    | None – Table IDs of the SIP Error Treatment tables  |

For more information on the parameters, see the topic **Add BGCF Profile Attribute** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

**6 Click OK.**

**Result:** The BGCF Profile table attributes are provisioned successfully.

.....  
**END OF STEPS**.....

# To provision BGCF Time Of Day

## Purpose

This procedure is used provision BGCF Time Of Day table parameters that are used to determine BGCF routing.

## Before you begin

Observe the following:

- BGCF Network Gateway table is already provisioned
- BGCF Default Network Gateway table is already provisioned
- Target List ID is already provisioned

This screen is used to define the TOD routing information. TOD routing is used during traditional BGCF DA routing (as a Time Of Day Id can be associated with a BGCF DA entry). Up to 32 Time of Day tables can be defined.

## Frequency

This procedure must be performed to activate time of day routing.

## Required information

This procedure is performed at the Provisioning GUI.

## Steps to provision a BGCF Time Of Day table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS** → **IMS Components** → **BGCF Tables**.

**Result:** The **BGCF Tables** window is displayed.

---

- 2 In the left pane, expand the **BGCF Time Of Day** folder.

**Result:** The BGCF Time Of Day tables are listed under the folder in the left pane.

If the folder is empty, add a BGCF Time Of Day table.

Perform the following steps in the **BGCF Tables** window to add, rename, or delete a BGCF Time Of Day table :

| If you want to ...               | then ...  |
|----------------------------------|---|
| add a BGCF Time Of Day table,    | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a BGCF Time Of Day table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a BGCF Time Of Day table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a BGCF Time Of Day table, ensure that no table entries are in use.</p> <p><i>End of steps</i></p>  |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the BGCF Time Of Day table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **BGCF Tables** window to add, modify, or delete the BGCF Time Of Day table attributes:

| If you want to ...                          | then ...  |
|---|---|
| add the BGCF Time Of Day table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a BGCF Time Of Day table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a BGCF Time Of Day table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>           |

- 5 Provision the following parameters:

| Parameter                    | Provisioning  |
|------------------------------|---|
| <b>BGCF Routing Interval</b> | In the <b>BGCF Routing Interval</b> area of the screen, select the interval start <b>date</b> and <b>time</b> from the menu and then the interval end <b>date</b> and <b>time</b> . |

| Parameter                         | Provisioning  |
|-----------------------------------|---|
| <b>Target List Id</b>             | From the menu in the <b>Target List Id</b> field, select a predefined Target list table that is used to route the call. This field is mutually exclusive with the <b>NGW/DNGW IDs</b> . This is a drop-down selection pre-populated with the defined Target list Ids. |
| <b>Network Gateway Id</b>         | From the menu in the <b>Network Gateway Id</b> field, select the predefined BGCF Network Gateway that is used to route the call. This field is mutually exclusive with the <b>Target List ID</b> .  |
| <b>Default Network Gateway Id</b> | From the menu in the <b>Default Network Gateway Id</b> field, select the predefined BGCF Default Network Gateway that is used to route the call. This field is mutually exclusive with the <b>Target List ID</b> .  |

For more information on the parameters, see the topic **BGCF Time of Day Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click **OK**.

**Result:** The BGCF Time Of Day table attributes are provisioned successfully.

END OF STEPS

---

# To provision BGCF Network Gateway

## Purpose

This procedure is used to provision a BGCF Network Gateway.

## Reason to create a BGCF Network Gateway (NGW) routing table

This screen is used to define the NGW routing information.

NGW routing is used during:

- Originating Host Class routing
- Subscriber routing
- Traditional BGCF DA routing

To select an NGW route, the NGW Id is used to select the proper NGW Table, then the dialed digits are used to select the proper route.

There can be up to 32 NGW Tables defined and each NGW table can have up to 128 entries.

## Before you *delete* a BGCF Network Gateway routing table

Before you *delete* a BGCF Network Gateway routing table, Ensure that no BGCF Network Gateway routing table are used in BGCF routing.

## Before you begin

Observe the following:

- This procedure must be performed whenever a BGCF Network Gateway routing table must be provisioned.
- This procedure is performed at the Provisioning GUI.

## Steps to provision a BGCF Network Gateway table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS** → **IMS Components** → **BGCF Tables**.

**Result:** The **BGCF Tables** window is displayed.

- 
- 2 In the left pane, expand the **BGCF Network Gateway** folder.

**Result:** The BGCF Network Gateway tables are listed under the folder in the left pane.

If the folder is empty, add a BGCF Network Gateway table.

Perform the following steps in the **BGCF Tables** window to add, rename, or delete a BGCF Network Gateway table :

| If you want to ...                   | then ...   |
|--------------------------------------|--|
| add a BGCF Network Gateway table,    | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/> <b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a BGCF Network Gateway table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/> <b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a BGCF Network Gateway table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a BGCF Network Gateway table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>  |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the BGCF Network Gateway table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **BGCF Tables** window to add, modify, or delete the BGCF Network Gateway table attributes:

| If you want to ...                              | then ...  |
|---|---|
| add the BGCF Network Gateway table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol>   |
| modify a BGCF Network Gateway table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol> |
| delete a BGCF Network Gateway table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.<br/><i>End of steps.</i></li> </ol>           |

- 5 Provision the following parameters:

| Parameter                 | Provisioning  |
|---------------------------|---|
| <b>Network Gateway ID</b> | Enter a unique number from 1 to 999 to identify this table in the <b>Network Gateway ID</b> . |

| Parameter                    | Provisioning  |
|------------------------------|---|
| <b>Dialed Number Range</b>   | Enter a 1-16 digit dialed number in the <b>Dialed Number Range</b> field.<br><br><b>Note:</b> The Dialed Number Range field can contain *, #, x, &, 0-9, + and Hex digits. + is allowed at the beginning of the digits.                 |
| <b>Routing Prefix Digits</b> | If desired, enter 1-11 digits in the <b>Routing Prefix Digits</b> field. This digit routing prefix is used when routing calls.<br><br><b>Note:</b> The Routing Prefix Digits field can contain *, #, x, &, 0-9, + and Hex digits.       |
| <b>Prefix Digits</b>         | If desired, enter 1-11 digits in the <b>Prefix Digits</b> field. This routing prefix is used when routing calls.<br><br><b>Note:</b> The Prefix Digits field can contain *, #, x, &, 0-9, + and Hex digits.                             |
| <b>Suffix Digits Length</b>  | Enter number of digits that is used from the original R-URI in the <b>Suffix Digits Length</b> field. If the number of suffix digits is greater than the number of digits in the original R-URI, then all digits in the R-URI are used. |
| <b>Target List Id</b>        | Select the list of routes from the menu in the <b>Target List Id</b> field. This Id is used for routing calls.  |

For more information on the parameters, see the topic **BGCF Network Gateway Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

6 Click **OK**.

**Result:** The BGCF Network Gateway table attributes are provisioned successfully.

END OF STEPS

# To provision BGCF Default Network Gateway

## Purpose

This procedure is used to provision a BGCF Default Network Gateway routing table.

## Reason to create a BGCF Default Network Gateway (NGW) routing table

This screen is used to define the Default NGW routing information.

NGW routing is used during:

- Originating Host Class routing
- Subscriber routing
- Traditional BGCF DA routing

To select a Default NGW route, the Default NGW ID is used. Up to 32 Default NGW entries can be defined.

## Before you *delete* a BGCF Default Network Gateway routing table

Before you *delete* a BGCF Default Network Gateway routing table, you must ensure that no BGCF Default Network Gateway routing table is used in BGCF routing.

## Before you begin

Observe the following:

- This procedure must be performed whenever a BGCF Default Network Gateway routing table must be provisioned.
- This procedure is performed at the Provisioning GUI.

## Steps to provision a BGCF Default Network Gateway table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS → IMS Components → BGCF Tables**.

**Result:** The **BGCF Tables** window is displayed.

- 
- 2 In the left pane, expand the **BGCF Default Network Gateway** folder.

**Result:** The BGCF Default Network Gateway tables are listed under the folder in the left pane.

If the folder is empty, add a BGCF Default Network Gateway table.

Perform the following steps in the **BGCF Tables** window to add, rename, or delete a BGCF Default Network Gateway table :

| If you want to ...                           | then ...  |
|--|---|
| add a BGCF Default Network Gateway table,    | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a BGCF Default Network Gateway table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a BGCF Default Network Gateway table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a BGCF Default Network Gateway table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>                                   |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the BGCF Default Network Gateway table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **BGCF Tables** window to add, modify, or delete the BGCF Default Network Gateway table attributes:

| If you want to ...                                      | then ...  |
|---|---|
| add the BGCF Default Network Gateway table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a BGCF Default Network Gateway table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a BGCF Default Network Gateway table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>           |

- 5 Provision the following parameters:

| Parameter                         | Provisioning  |
|-----------------------------------|---|
| <b>Default Network Gateway ID</b> | Enter a unique number to identify this table in the <b>Default Network Gateway ID</b> field.<br><b>Note:</b> The available values are 1-32. |
| <b>Description</b>                | Type a unique (descriptive) name in the <b>Description</b> field.   |

| Parameter                    | Provisioning   |
|------------------------------|--|
| <b>Routing Prefix Digits</b> | If desired, enter 1-11 digits in the <b>Routing Prefix Digits</b> field. This digit routing prefix is used when routing calls.<br><br><b>Note:</b> The Routing Prefix Digits field can contain *, #, x, &, 0-9, + and Hex digits.                |
| <b>Prefix Digits</b>         | If desired, enter 1-11 digits in the <b>Prefix Digits</b> field. This routing prefix is used when routing calls.<br><br><b>Note:</b> The Prefix Digits field can contain *, #, x, &, 0-9, + and Hex digits.                                      |
| <b>Suffix Digits Length</b>  | Enter the number of digits that will be used from the original R-URI in the <b>Suffix Digits Length</b> field. If the number of suffix digits is greater than the number of digits in the original R-URI, then all digits in the R-URI are used. |
| <b>Target List Id</b>        | Select the list of routes from the menu in the <b>Target List Id</b> field. This ID is used for routing calls.   |

For more information on the parameters, see the topic **BGCF Default Network Gateway Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

**6** Click **OK**.

**Result:** The BGCF Default Network Gateway table attributes are provisioned successfully.

END OF STEPS

# To provision Originating Host Class Profile routing for BGCF

## Purpose

This procedure is used for provisioning an Originating Host Class Profile to define parameters that are used to determine BGCF routing.

## Originating Host Class Profile routing

This profile is used to associate a Network Gateway (NGW) table ID and/or a Default Network Gateway (NGW) table ID with an originating class. A maximum of 512 entries are supported in this table.

## Originator class analysis

Subscriber/Originating Host class profile routing must be activated to provide this functionality.

## Before you begin

Observe the following:

- BGCF Network Gateway table is already provisioned
- BGCF Default Network Gateway table is already provisioned
- This procedure must be performed to activate Originating host class profile routing for BGCF

## Steps to create a BGCF originating host class profile

Perform the following at the Provisioning GUI:

- 
- 1 Select **IMS** → **IMS Components** → **BGCF Tables**.

---

  - 2 In the left pane, expand the **BGCF Originating Host Class Profile**.
-

| 3 | If you want to                                | Then  |
|---|---|---|
|   | Add a BGCF Originating Host Class profile,    | <ol style="list-style-type: none"> <li>Right click and select <b>Add Table</b>.<br/><b>Result:</b> The <b>Add BGCF Originating Host Class Profile</b> window is displayed.</li> <li>Select the table number from the drop down list and enter a table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><b>Result:</b> The BGCF Originating Host Class profile table is successfully added.</p> |
|   | Modify a BGCF Originating Host Class profile, | <p>Select the table you want to rename, then select <b>Rename Table</b> from the Tables menu.</p> <p>Rename the table and Click <b>OK</b>.</p> <p>End of procedure.</p>   |
|   | Delete a BGCF Originating Host Class profile, | <p>Select the BGCF table you want to delete, then select <b>Delete Table</b> from the Tables menu.</p> <p>Click <b>OK</b>.</p> <p>Note: BGCF originating host class profile can only be deleted when all references to the BGCF originating host class profile have been removed.</p> <p>End of procedure.</p>  |

4 Double-click on the specific BGCF Originating Host Class profile table. Select **Attributes** → **Add Table Attributes** from the menu.

5 Provision the following parameters in the **BGCF Originating Host Class Profile** window:

| Parameter                         | Provisioning  |
|-----------------------------------|---|
| <b>Host Class</b>                 | Type a unique numerical characters to indicate the value in the class associated with the <b>Originating Host list</b> .  |
| <b>Network Gateway Id</b>         | Select the BGCF Network Gateway that is used to route the call from the drop down list.   |
| <b>Default Network Gateway Id</b> | Select the BGCF Default Network Gateway that is used to route the call from the drop down list. This field is mutually exclusive with the <b>Target List ID</b> . |
| <b>Country Indicator</b>          | Select <b>US</b> or <b>non-US</b> in this field.  |

- 
- 6 Click OK.

**Result:** A subscriber profile is created.

END OF STEPS

---

# To provision Subscriber Profile routing for BGCF

## Purpose

This procedure is used to provision Subscriber Profile routing for BGCF.

## Subscriber Profile routing

The Subscriber/Originating Class Profile routing must be turned on to activate Subscriber Profile routing functionality. When routing is based on the Subscriber Profile, extensive digit manipulation must be performed based on subscriber data as well as Local/Toll analysis. The selection of which route to take is based on this analysis. BGCF also needs to determine the availability of a route before the route is attempted.

## Originator class analysis

When a call comes into the BGCF and if no class parameter exists in the Req-URI, the Originating Subscriber ID from the P-Asserted ID parameter is checked. This information is looked up in the Subscriber Profile table. If a match exists, the routing information related to this Subscriber ID is retrieved and the call is routed based on this information.

## Before you begin

Observe the following:

- Network Gateway (NGW) is already provisioned.
- Default Network Gateway (DNGW) is already provisioned.
- SLG is already provisioned.
- This procedure is performed at the Provisioning GUI.

## Create a rate center to office ID

An **Office ID** must be defined and is used to normalize the Rate Center and State information. The **Office ID** is used during subscriber routing of US calls for the determination of local/toll.

Perform the following at the Provisioning GUI:

- 
- 1 Select **IMS → IMS Components → BGCF Tables → BGCF Rate Center to Office Id**.

---

  - 2 Right-click on **BGCF Rate Center to Office Id** and select **Add Table**.

---

  - 3 Select a table number from the drop down list and type a table name. Click **OK**.

**Result:** A BGCF Rate Center to Office Id table is created successfully.

- 4 Double-click on the BGCF Rate Center to Office Id table created. Select **Attributes → Add Table Attributes** from the menu.
  
- 5 Provision the following parameters in the **BGCF Rate Center to Office Id** window:

| Parameter          | Provisioning  |
|--------------------|---|
| <b>Rate Center</b> | Enter an identification character in this field. The identification can contain 1 to 10 characters.   |
| <b>State</b>       | Select the location of the rate center from the drop down list.                                       |
| <b>Office Id</b>   | Enter a value between 1 - 999 to indicate that it is associated with the input Rate Center and State. |

- 6 Click **OK**.

END OF STEPS

### To create a BGCF Office Codes table

A BGCF Office Codes table must be defined and is used to associate an NPA-NXX with an Office ID (Rate Center and State) and a LATA. The Office Code data is used during subscriber routing of US calls for the determination of local/toll.

Perform the following at the Provisioning GUI:

- 1 Select **IMS → IMS Components → BGCF Tables → BGCF Office Codes**.
  
- 2 Create a BGCF Office Codes table.
  
- 3 Double-click on the BGCF Office Codes table created. Select **Attributes → Add Table Attributes** from the menu.

**4**

| Parameter | Provisioning   |
|-----------|--|
| NPA       | Enter a value.   |
| NXX       | Enter a value.   |
| Office Id | From the drop down list, select the value that is associated with the input Rate Center and State in which the NPA-NXX is located. |
| LATA      | Enter the table in which the NPA-NXX is located.   |

**5** Click **OK**.

E N D O F S T E P S

**To create a BGCF local area calling information table**

A BGCF local area calling information table must be defined and is used to determine local calling areas. When an entry is made in this table, it indicates that calls from the **Originating Office Id** to the **Terminating Office Id** are considered local during subscriber routing of US calls.

Perform the following at the Provisioning GUI:

**1** Select **IMS → IMS Components →BGCF Tables → BGCF Local Calling Area Info**.**2** Create a BGCF Local Calling Area Info table.**3** Double-click on the BGCF Local Calling Area Info created. Select **Attributes → Add Table Attributes** from the menu.**4** Provision the following parameters in the **BGCF Local Calling Area Info** window:

| Parameter             | Provisioning                            |
|-----------------------|---|
| Originating Office Id | Select a value from the drop down list. |
| Terminating Office Id | Select a value from the drop down list. |

- 
- 5 Click OK.

END OF STEPS

---

## To create a BGCF directory assistance table

A BGCF directory assistance table must be defined and is used to add Directory Assistance Numbers to the Directory Assistance table. Each table can have up to 20 entries in addition to the default pre-populated entries. There can be a maximum number of 16 Directory Assistance tables defined. This information is used during subscriber routing if a subscriber entry has a **Directory Table Id** identified.

Perform the following at the Provisioning GUI:

---

- 1 Select **IMS → IMS Components → BGCF Tables**.

---

- 2 In the left pane, expand the **BGCF Directory Assistance** folder.

---

- 3 Right click **BGCF Directory Assistance** and select **Add Table** from the menu.

---

- 4 Double-click on the BGCF Directory Assistance created. Select **Attributes → Add Table Attributes** from the menu.

**Result:** The **BGCF Directory Assistance Number** window is displayed.

---

- 5 Enter a valid number in the **Directory Assistance Number** field.

When defining a new table, it is pre-populated with three default entries as follows: **411**, **x411**, and **xxx5551212**. These defaults may be removed by the operator as needed.

**Note:** The Directory Assistance number field can contain \*, #, x, &, 0-9, and Hex digits. “x” is a wild card that matches any one digit.

---

- 6 Click OK.

END OF STEPS

---

## To create a BGCF Shared Local Gateway routing table

A Shared Local Gateway routing table must be defined. SLG routing is used during subscriber routing of US local calls. SLG routing is also used for subscriber routing of US toll calls destined to a CIC that is not in the Service Provider table. The Shared Local Gateway table can have up to 1024 entries.

To select an SLG route during the subscriber routing, a match of the subscriber provisioned **PIC/LPIC**, **CLLI**, and **Routing Prefix Digits** must occur with an entry in the SLG table. If a particular field such as **CLLI** is set to **None** in both the subscriber and SLG, then that would be considered a match of CLLI. For a routing match to occur, ALL three fields must match. Perform the following at the Provisioning GUI:

- 1 Select **IMS → IMS Components → BGCF Tables → BGCF Shared Local Gateway Routing**.
- 2 In the left pane, expand the **BGCF Shared Local Gateway Routing** folder.
- 3 Right click **BGCF Shared Local Gateway Routing** and select **Add Table** from the menu.
- 4 Double-click on the BGCF Shared Local Gateway Routing table created. Select **Attributes → Add Table Attributes** from the menu.

**Result:** The **BGCF Shared Local Gateway Routing** window is displayed.
- 5 Provision the following parameters in the **BGCF Shared Local Gateway Routing** window:

| Parameter                    | Provisioning  |
|------------------------------|---|
| <b>CIC</b>                   | Enter the four digit Carrier Inter-exchange Code for the SLG route in this field.<br><b>Note:</b> The CIC is the only field allowed to have wild card in the SLG table.   |
| <b>CLLI</b>                  | Type 11 character Common Language Location Identifier that identifies the switch in the field.  |
| <b>Routing Prefix Digits</b> | Type 1-11 digits in the field that are used when routing calls. These digits are prefixed to the original R-URI.<br><b>Note:</b> The Routing Prefix Digits field can contain *, #, x, &, 0-9, + and Hex digits. |

| Parameter                   | Provisioning   |
|-----------------------------|--|
| <b>Suffix Digits Length</b> | Enter the number of digits that are used from the original R-URI in the field. These digits are appended to the Routing Prefix Digits.<br><br><b>Note:</b> If the number of suffix digits is greater than the number of digits in the original R-URI, then all digits in the R-URI are used. |
| <b>Target List Id</b>       | Select the list of routes that are used for routing the call from the drop down.   |

- 6 Click **OK**.

END OF STEPS

#### To create a BGCF Service Provider CIC table

A Service Provider CIC table must be defined and is used to define the CICs of the service provider. This table shall support up to 128 entries. This table is used during subscriber routing as one factor in the determination of SLG or NGW routing.

Perform the following at the Provisioning GUI:

- 1 Select **IMS → IMS Components → BGCF Tables → BGCF Service Provider CIC**.
- 2 Select the specific BGCF Service Provider CIC table and select **Attributes → Add Table Attributes**.
- 3 Enter the four digit Carrier Inter-exchange Code for the service provider in the **Service Provider CIC** field.  
  
**Note:** Wild cards are allowed for this field.
- 4 Click **OK**.

END OF STEPS

## To create a BGCF Subscriber Profile

Perform the following at the Provisioning GUI:

- 1 Select **IMS → IMS Components → BGCF Tables**.

- 2 In the left pane, expand the **BGCF subscriber profile** folder.

| 3 | If you want to                    | Then  |
|---|-----------------------------------|---|
|   | add a BGCF subscriber profile,    | <ol style="list-style-type: none"> <li>1. Select <b>Table → Add Table Attributes</b>.<br/><b>Result:</b> The <b>Add BGCF Subscriber Profile</b> table window is displayed.</li> <li>2. Select the table number from the drop down list and enter the table name.</li> <li>3. Click <b>OK</b>.<br/><i>End of steps</i></li> </ol>                              |
|   | modify a BGCF subscriber profile, | <ol style="list-style-type: none"> <li>1. Select the table you want to modify.</li> <li>2. Right-click and select <b>Rename Table</b></li> <li>3. Modify the name and click <b>OK</b>.<br/><i>End of procedure.</i></li> </ol>  |
|   | delete a BGCF subscriber profile, | <ol style="list-style-type: none"> <li>1. Select the table you want to delete.</li> <li>2. Right-click and select <b>Delete Table</b>.</li> <li>3. Click <b>OK</b> to confirm deletion.<br/><i>End of procedure.</i></li> </ol> <p><b>Note:</b> Before you delete a BGCF subscriber profile table, ensure the table is not used by any other BGCF tables.</p> |

- 4 Double-click on the specific **BGCF Subscriber Profile** table. Select **Attributes → Add Table Attributes** from the menu.

- 5 Provision the following parameters in the **BGCF Subscriber Profile** window:

| Parameter            | Provisioning  |
|----------------------|---|
| <b>Subscriber ID</b> | Enter the unique subscriber identifier in the form user@host in this field. |

| Parameter                         | Provisioning  |
|-----------------------------------|---|
| <b>Country Indicator</b>          | Select either US or Non-US from the drop down list.   |
| <b>PIC</b>                        | Enter the four digit Inter-LATA toll Primary Inter-exchange Carrier of the subscriber in this field.<br><b>Note:</b> This field is mandatory when the Country Indicator is US.  |
| <b>LPIC</b>                       | Enter the four digit Intra-LATA toll Primary Inter-exchange Carrier of the subscriber in this field.<br><b>Note:</b> This field is mandatory when the Country Indicator is US.  |
| <b>CLLI</b>                       | If desired, enter the 11 character Common Language Location Identifier that identifies the switch associated with the subscriber in this field.   |
| <b>Routing Prefix Digits</b>      | If desired, enter the 1-11 digit routing prefix in this field. This value is used when routing calls from this subscriber.<br><b>Note:</b> The Routing Prefix Digits field can contain *, #, x, &, 0-9, + and Hex digits. |
| <b>Directory Assistance Id</b>    | If assigned, select the from the menu to indicate the Directory Assistance Table used for routing if the call is a directory assistance call.   |
| <b>Network Gateway Id</b>         | Select a value from the drop down list.   |
| <b>Default Network Gateway Id</b> | Select a value from the drop down list.   |

- 6 Click OK.

**Result:** A subscriber profile is created.

END OF STEPS

### To activate Subscriber Profile routing

Perform the following at the Provisioning GUI:

- 1 Select **IMS → Parameters/timers → BGCF parameters**.

**2** Provision the following parameters in the **BGCF Parameters** window:

| Parameter   | Provisioning  |
|---|---|
| <b>Subscriber/Originating Class Profile Routing</b> | Select the check box.   |
| <b>Add 1 Prefix for US Calls</b>                    | <p>By selecting this check box, a prefix of <b>1</b> is added to the destination number before routing the call if:</p> <ul style="list-style-type: none"> <li>• Subscriber/Originating Class Profile Routing is enabled.</li> <li>• Call is a toll call.</li> <li>• The destination number is 10 digits and the subscriber country is US.</li> </ul>   |
| <b>Remove 011 for International Calls</b>           | <p>By selecting this check box, the BGCF removes the <b>011</b> (if present) before routing the call, if:</p> <ul style="list-style-type: none"> <li>• Subscriber/Originating Class Profile Routing is enabled.</li> <li>• Call is a toll call.</li> </ul> <p><b>Note:</b> If both the <b>Remove 011 for International Calls</b> indicator and the <b>Add 1 Prefix for US Calls</b> indicator are set, then the <b>011</b> is removed first and then the <b>1</b> is added.</p> |
| <b>Remove P-Media Authorization</b>                 | By selecting this check box, the P-Media Authorization header is removed in case it exists.   |
| <b>Routing Based on SDP Media Type</b>              | Select the check box based on the user requirement.<br><b>Note:</b> This is not a mandatory field.  |
| <b>Location Based Routing</b>                       | Select the check box based on the user requirement.<br><b>Note:</b> This is not a mandatory field.  |
| <b>Calling Party Identity</b>                       | Select the value from the drop down list.<br><b>Note:</b> This is not a mandatory field.  |

**3** Click **OK**.

**Result:** BGCF subscriber profile routing is activated

END OF STEPS

# To provision BGCF DA Route Table

## Purpose

This procedure is used to provision a BGCF Digit Analysis (DA) Route Table.

## Before you **delete** a BGCF DA Route Table

Before you *delete* a BGCF DA Route Table, ensure that the table is not used by a BGCF profile.

## Before you begin

Observe the following:

- BGCF Target URI is already provisioned.
- BGCF Target URI-QPriority List is already provisioned.
- Time of day table, NGW and DNGW tables must be populated before the DA Routing table is populated
- Default routing on BGCF incorporates Time of Day routing. Routing takes precedence for Time-Of-Day provisioning. Calls are routed through provisioned target list only if no match exists in Time-Of-Day table or if the Time-Of-Day table is not provisioned.
- Both the **Network Gateway Id** and the **Default Network Gateway Id** can be populated. In this case, the routes designated by the NGW Table are attempted first and if the routes fail, the routes designated by the DNGW Table are attempted.
- This procedure must be performed whenever a BGCF DA Route Table must be added, modified, or deleted.
- This procedure is performed at the FS GUI.

## Steps to provision a BGCF DA Route Table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS** → **IMS Components** → **BGCF Tables**.

**Result:** The **BGCF Tables** window is displayed.

- 
- 2 In the left pane, expand the **BGCF DA Route Table** folder.

**Result:** The BGCF DA Route Table tables are listed under the folder in the left pane.

If the folder is empty, add a BGCF DA Route Table.

Perform the following steps in the **BGCF Tables** window to add, rename, or delete a BGCF DA Route Table :

| If you want to ...            | then ...  |
|-------------------------------|---|
| add a BGCF DA Route Table,    | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a BGCF DA Route Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a BGCF DA Route Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a BGCF DA Route Table, ensure that no table entries are in use.</p> <p><i>End of steps</i></p>   |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the BGCF DA Route Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **BGCF Tables** window to add, modify, or delete the BGCF DA Route Table attributes:

| If you want to ...                       | then ...  |
|--|---|
| add the BGCF DA Route Table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a BGCF DA Route Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a BGCF DA Route Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>           |

- 5 Provision the following parameters:

| Parameter | Provisioning   |
|-----------|--|
| DN Type   | Select <b>Calling Number</b> or <b>Called Number</b> in the <b>DN Type</b> . |

| Parameter                              | Provisioning  |
|--|---|
| <b>Calling Number or Called Number</b> | <p>Enter the digit strings that are matched with the digit strings received in the request message in the <b>Calling Number or Called Number</b> field.</p> <p><b>Note:</b> For Called Number, the digit string can contain *, #, x, &amp;, 0-9, + and Hex digits.</p>  |
| <b>Target List ID</b>                  | Select the target list in the <b>Target List ID</b> field. This Id will be used to create dynamic next-hop list .   |
| <b>Criteria and Value</b>              | <p>Select <b>CIC</b> or <b>CdPN</b> in the <b>Criteria</b> and enter the associated value parameter in the <b>Value</b> attribute.</p> <p><b>Note:</b> This is only possible when Calling Number has been selected as DN Type. For value restrictions see the <i>Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual</i>, 275-900-379.</p> <p><b>Note:</b> You can enter the digit string with or without the “+” sign in the <b>Value</b> field. However, routing remains the same.</p> |
| <b>Time of Day ID</b>                  | If desired, select the <b>Time of Day ID</b> table from the menu. The TOD Table is checked to determine if alternate routing is be applied for this call. If the current time is not provisioned in the TOD Table, then the routing on this screen is used to route the call.   |
| <b>Network Gateway ID</b>              | <p>If desired, select a network gateway ID in the <b>Network Gateway ID</b> field.</p> <p><b>Note:</b> The NGW Table is used to route the call. This field is mutually exclusive with the <b>Target List ID</b>.</p>  |
| <b>Default Network Gateway ID</b>      | <p>If desired, select the default network gateway ID in the <b>Default Network Gateway ID</b> field.</p> <p><b>Note:</b> The DNGW Table is used to route the call. This field is mutually exclusive with the <b>Target List ID</b>.</p>   |
| <b>Digit Table Id</b>                  | Select the appropriate value of the digit table from the <b>Digit Table Id</b> list.  |

---

For more information on the parameters, see the topic **Add DA Route Table Attributes** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

---

- 6 Click OK.

**Result:** The BGCF DA Route Table attributes are provisioned successfully.

END OF STEPS

---

# To provision BGCF SIP content type

## Purpose

This procedure is used to provision a BGCF SIP content type table.

The BGCF SIP content type table allows the BGCF to route SIP MESSAGE requests differently from other types of SIP requests (such as INVITE and OPTION). Additionally, the BGCF can route SIP MESSAGE requests to different destinations according to their Content-type header.

This feature can be used by all types of SIP MESSAGE requests, such as

- Short Message Service (SMS)
- Instant Message (IM)
- Unstructured Supplementary Service Data (USSD).

If no entries are contained in the BGCF SIP Content Type table or no BGCF SIP Content Type table is provisioned, this feature is treated as being disabled.

## Before you begin

Observe the following:

### Frequency

This procedure is performed whenever an SIP content type table must be provisioned.

### Required information

This procedure is performed at the Provisioning GUI.

## Steps to provision a BGCF SIP Content Type table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select IMS → IMS Components →BGCF Tables.

**Result:** The BGCF SIP Content Type window is displayed.

---

- 2 In the left pane, expand the **BGCF SIP Content Type** folder.

**Result:** The BGCF SIP Content Type tables are listed under the folder in the left pane.

If the folder is empty, add a BGCF SIP Content Type table.

Perform the following steps in the **BGCF SIP Content Type** window to add, rename, or delete a BGCF SIP Content Type table :

| If you want to ...                    | then ...  |
|---------------------------------------|---|
| add a BGCF SIP Content Type table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>BGCF SIP Content Type</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a BGCF SIP Content Type table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>BGCF SIP Content Type</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |
| delete a BGCF SIP Content Type table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a BGCF SIP Content Type table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>  |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the BGCF SIP Content Type table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **BGCF SIP Content Type** window to add, modify, or delete the BGCF SIP Content Type table attributes:

| If you want to ...                               | then ...  |
|--|---|
| add the BGCF SIP Content Type table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF SIP Content Type</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a BGCF SIP Content Type table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF SIP Content Type</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a BGCF SIP Content Type table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p>                      |

**5** Provision the following parameters:

| Parameter              | Provisioning   |
|------------------------|--|
| <b>Content Type</b>    | Populate the <b>Content Type</b> field with one of eight possible values identifying the type of content in the SIP MESSAGE request: text, image, audio, audio, video, application, message, multipart, or model.<br><br>A combination of the <b>Content Type</b> and <b>Content Subtype</b> fields is used to match the “Content Type” header string of the incoming SIP MESSAGE request.                                   |
| <b>Content Subtype</b> | Populate the <b>Content Subtype</b> field.<br><br>This field holds a maximum of 50 characters. Space is not a valid character.   |
| <b>Action</b>          | Select an <b>Action</b> type.<br><br>Possible values: <ul style="list-style-type: none"> <li>• RT (Route) - Route the SIP MESSAGE request according to the target list specified in the Target List ID field</li> <li>• DA (Digit Analysis) - Route the SIP MESSAGE request using existing call logic, such as CIC + Calling number</li> <li>• RJ (Reject) - Reject the SIP MESSAGE request with 403 (Forbidden).</li> </ul> |
| <b>Target List Id</b>  | Select a <b>Target List Id</b> .<br><br>The Target List ID selection is populated with IDs that have been provisioned under BGCF Target List table.  |

For more information on the parameters, see the topic **BGCF SIP Content Type Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

**6** Click **OK**.

**Result:** The BGCF SIP Content Type table attributes are provisioned successfully.

END OF STEPS

# To provision BGCF local number routing

## Purpose

This procedure is used to provision BGCF local number routing. To support local number routing capability, a BGCF local number Digit Analysis table and a BGCF local number routing table needs to be defined.

The presence of a BGCF Originating Source Info Table is optional. This table is used to find the associated Local Number Routing Table according to the originating information from the incoming SIP INVITE message.

## Before you begin

Observe the following:

- BGCF Target URI is already provisioned
- BGCF Target URI-QPriority List is already provisioned
- Time of day table, NGW, and DNGW tables is populated before the DA Routing table is populated
- Default routing on BGCF incorporates Time of Day routing. Routing takes precedence for Time-Of-Day provisioning. Calls are routed using the provisioned target list only if no match in the Time-Of-Day table or if the Time-Of-Day table is not provisioned.
- Both the **Network Gateway Id** and the **Default Network Gateway Id** are populated. In that case, the routes designated by the NGW Table are attempted first, and then if those routes fail, the routes designated by the DNGW Table are attempted.

## Frequency

This procedure must be performed when either one of the following updates apply:

- Add, modify, or delete a BGCF Local Number Digit Analysis table
- Assign a Phone-Context parameter to a BGCF Local Number Digit Analysis table to support local number routing

## Steps to provision BGCF Local Number DA table

Perform the following at the Provisioning GUI:

- 
- 1 Select **IMS → IMS Components → BGCF Tables** and in the left pane, expand the **BGCF Local Number DA**.

**Note:** If no BGCF Local Number DA table is provisioned, then add a new table.

| 2 | If you want to                                  | Then   |
|---|---|--|
|   | add a BGCF local number DA table,               | <p>do the following:</p> <ol style="list-style-type: none"> <li>1. Right-click on <b>BGCF local number DA</b> and select <b>Add Table</b>.</li> <li>2. Provide a <b>Table Number</b> and a <b>Table Name</b> in the <b>Add BGCF local number DA table</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>   |
|   | modify (= rename) a BGCF local number DA table, | <ol style="list-style-type: none"> <li>1. Select the table you want to modify.</li> <li>2. Right-click and select <b>Rename Table</b></li> <li>3. Modify the name and click <b>OK</b>.</li> </ol> <p><i>End of procedure.</i></p>  |
|   | delete a BGCF local number DA table,            | <ol style="list-style-type: none"> <li>1. Select the table you want to delete.</li> <li>2. Right-click and select <b>Delete Table</b>.</li> <li>3. Click <b>OK</b> to confirm deletion.</li> </ol> <p><i>End of procedure.</i></p> <p><b>Note:</b> Before you delete a BGCF local number DA table, ensure that the table is not used by any local number routing tables.</p> |

- 3 Double click the desired BGCF local number DA table.

**Result:** The BGCF local number DA table attributes screen appears on the right-pane window.

- 4 Right click a value from the table and:

| If you want to ...                                 | Then ...   |
|--|--|
| add attributes to a BGCF local number DA table,    | <p>Right-click on the BGCF local number DA table attributes screen, and select <b>Add Table Attribute</b>.</p> <p><b>Result:</b> The <b>BGCF local number DA</b> screen appears.</p>   |
| modify attributes of a BGCF local number DA table, | <p>Right-click the desired BGCF local number DA and click <b>Modify Table Attribute</b>.</p> <p><b>Result:</b> The <b>BGCF local number DA</b> screen appears.<b>Note:</b> DN Type and Called Number cannot be modified.</p> |

| If you want to ...                                | Then ...   |
|---|--|
| delete attributes of a BGCF local number DA table | <ol style="list-style-type: none"> <li>Right-click the desired BGCF local number DA and click <b>Delete Table Attribute</b>.</li> <li>Click <b>Ok</b> to confirm deletion.</li> </ol> <p><i>End of procedure</i></p> |

- 5 Provision the following parameters in the **Bgcf Local Num DA Attributes** window:

| Parameter                              | Provisioning   |
|--|--|
| <b>DN Type</b>                         | Select one of the available values <b>Calling Number</b> or <b>Called Number</b> from the drop down list.  |
| <b>Calling Number or Called Number</b> | Enter the digit strings that match with the digit strings received in the request message.<br><b>Note:</b> For Called Number, the digit string can contain *, #, x, &, 0-9, + and Hex digits.  |
| <b>Target List ID</b>                  | Select the target list that is used to create dynamic next-hop list.   |
| <b>Criteria</b>                        | Select the values <b>CIC</b> or <b>CdPN</b> from the drop down.  |
| <b>Value</b>                           | Enter the associated value parameter in the attribute.<br><b>Note:</b> The associated value parameter can be entered only when the Calling Number has been selected as DN Type. For value restrictions, see <i>Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual</i> , 275-900-379. |
| <b>Time of Day ID</b>                  | Select the specific table from the menu.<br><b>Note:</b> If the TOD Table is checked, then alternate routing for the call is applied. If the current time is not provisioned in the TOD Table, then the routing on this screen is used to route the call.  |
| <b>Network Gateway ID</b>              | Select the specific gateway Id from the menu.<br><b>Note:</b> The NGW Table is used to route the call. This field is mutually exclusive with the <b>Target List ID</b> .   |
| <b>Default Network Gateway ID</b>      | Select the specific gateway Id from the menu.<br>The DNGW Table is used to route the call. This field is mutually exclusive with the <b>Target List ID</b> .   |

- 6 Click **OK**.

**Result:** A BGCF Local Number DA table attribute is added or modified.

END OF STEPS

### Steps to provision BGCF Local Number Routing table

**Note:** The BGCF Local Number DA table must be added first before adding the BGCF Local Number Routing table.

Perform the following at the Provisioning GUI:

- 1 Select **IMS → IMS Components → BGCF Tables** and in the left pane, expand the **BGCF Local Number Routing**.

**Note:** If no BGCF Local Number Routing table is provisioned, then add a new table.

| 2 | If you want to                                       | Then   |
|---|--|--|
|   | add a BGCF local number Routing table,               | <p>do the following:</p> <ol style="list-style-type: none"> <li>1. Right-click on <b>BGCF local number Routing</b> and select <b>Add Table</b>.</li> <li>2. Provide a <b>Table Number</b> and a <b>Table Name</b> in the <b>Add BGCF local number Routing</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>   |
|   | modify (= rename) a BGCF local number Routing table, | <ol style="list-style-type: none"> <li>1. Select the table you want to modify.</li> <li>2. Right-click and select <b>Rename Table</b></li> <li>3. Modify the name and click <b>OK</b>.</li> </ol> <p><i>End of procedure.</i></p>  |
|   | delete a BGCF local number Routing table,            | <ol style="list-style-type: none"> <li>1. Select the table you want to delete.</li> <li>2. Right-click and select <b>Delete Table</b>.</li> <li>3. Click <b>OK</b> to confirm deletion.</li> </ol> <p><i>End of procedure.</i></p> <p><b>Note:</b> BGCF local number Routing table can be deleted only when all references to the table have been removed.</p> |

- 3 Double click on the desired **BGCF Local Number Routing Table**.

**Result:** The BGCF Local Number Routing table attributes screen appears on the right-pane window.

- 4 Right click a value from the table and:

| If you want to ...                                      | Then ...   |
|---|--|
| add attributes to a BGCF Local Number Routing table,    | Right-click on the BGCF Local Number Routing table attributes screen and select <b>Add Table Attribute</b> .<br><b>Result:</b> The <b>BGCF Local Number Routing</b> screen appears.                                      |
| modify attributes of a BGCF Local Number Routing table, | Right-click the desired BGCF Local Number Routing and click <b>Modify Table Attribute</b> .<br><b>Result:</b> The <b>BGCF Local Number Routing</b> screen appears.   |
| delete attributes of a BGCF Local Number Routing table  | <ol style="list-style-type: none"> <li>1. Right-click the desired BGCF Local Number Routing and click <b>Delete Table Attribute</b>.</li> <li>2. Click <b>Ok</b> to confirm deletion.</li> </ol> <i>End of procedure</i> |

- 5 Provision the following parameters in the **BGCF Local Number Routing** window:

| Parameter                       | Provisioning  |
|---------------------------------|---|
| <b>Phone-Context</b>            | Enter the phone-context parameter to be used with the called DN for local number routing. |
| <b>Local Number DA Table ID</b> | Select a previously defined BGCF Local Number DA table from the drop down list.           |
| <b>Description</b>              | Enter a description of the table in this field.   |

- 6 Click **OK**.

**Result:** A BGCF Local Number Routing table attribute is added or modified.

END OF STEPS

**To provision BGCF Originating Source Info table**

**Note:** The BGCF Local Number Routing table must be added first before adding the BGCF Originating Source Info table.

Perform the following at the Provisioning GUI:

- 1 Select **IMS → IMS Components → BGCF Tables** and in the left pane, expand the **BGCF Originating Source Info**.

**Note:** If no BGCF Originating Source Info table is provisioned, then add a new table.

| 2 | If you want to  | Then  |
|---|---|---|
|   | add a BGCF Originating Source Info table,               | <ol style="list-style-type: none"> <li>1. Right-click on <b>BGCF Originating Source Info</b> and select <b>Add Table</b>.</li> <li>2. Provide a <b>Table Number</b> and a <b>Table Name</b> in the <b>Add BGCF Originating Source Info</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>   |
|   | modify (= rename) a BGCF Originating Source Info table, | <ol style="list-style-type: none"> <li>1. Select the table you want to modify.</li> <li>2. Right-click and select <b>Rename Table</b></li> <li>3. Modify the name and click <b>OK</b>.</li> </ol> <p><i>End of procedure.</i></p>   |
|   | delete a BGCF Originating Source Info table,            | <ol style="list-style-type: none"> <li>1. Select the table you want to delete.</li> <li>2. Right-click and select <b>Delete Table</b>.</li> <li>3. Click <b>OK</b> to confirm deletion.</li> </ol> <p><i>End of procedure.</i></p> <p><b>Note:</b> BGCF Originating Source Info table can be deleted only when all references to the table have been removed.</p> |

- 3 Double click the desired **BGCF Originating Source Info**.

**Result:** The BGCF Originating Source Info table attributes screen is displayed.

- 4 Right click a value from the table and:

| If you want to ...   | Then ...   |
|--|--|
| add attributes to a BGCF Originating Source Info table,    | <p>Right-click on the BGCF Originating Source Info table attributes screen and select <b>Add Table Attribute</b>.</p> <p><b>Result:</b> The <b>BGCF Originating Source Info</b> screen appears.</p>                                |
| modify attributes of a BGCF Originating Source Info table, | <p>Right-click the desired BGCF Originating Source Info and click <b>Modify Table Attribute</b>.</p> <p><b>Result:</b> The <b>BGCF Originating Source Info</b> screen appears.</p>   |
| delete attributes of a BGCF Originating Source Info table  | <ol style="list-style-type: none"> <li>1. Right-click the desired BGCF Originating Source Info and click <b>Delete Table Attribute</b>.</li> <li>2. Click <b>Ok</b> to confirm deletion.</li> </ol> <p><i>End of procedure</i></p> |

- 5 **Note:** The originating source depends on the value selected in the Source Type field.  
Enter the appropriate data in the **Originating Source** field:

| Source Type | Originating Source Value   |
|-------------|--|
| Domain      | A Domain string must be entered. “*” can be the wild card before a “.”. The star could indicate any character including empty character. When the “*” is an empty character, the “.” following the “*” is treated as an empty character. |
| IPv6        | An IPv6 address must be entered. The combination of this IP address and the value of the <b>Netmask</b> field is used for matching.  |
| IPv4        | An IPv4 address must be entered. The combination of this IP address and the value of the <b>Netmask</b> field is used for matching.  |
| Text String | Free format text string can be entered, and “&” can be entered at the end of the string as a wild card.  |

The Local Number Route Table associated with Local Number Route Table ID field is used to match the Phone Context information from the incoming SIP request if either one of the following conditions apply:

- The host information from the P-Asserted-ID header matches one of the entries in this table
- The host information from the From header matches one of the entries in this table

**6** Provision the following parameters:

| Parameter                       | Provisioning   |
|---------------------------------|--|
| <b>Local Num Route Table ID</b> | Select a previously defined Local Number Routing table from the drop down list.  |
| <b>Description</b>              | Enter a description of the table in this field.  |
| <b>Source Type</b>              | Select the originating source data type from the list.<br><b>Note:</b> The available values are <b>Domain</b> , <b>IPv4</b> , <b>IPv6</b> , and <b>Text String</b> . |
| <b>Netmask</b>                  | Enter the netmask for the IP address in this field.<br><b>Note:</b> The range for IPv4 is 0-32 and default is 32. The range for IPv6 is 0-128 and default is 128.    |

**7** Click OK.

**Result:** A BGCF Originating Source Info table attribute is added or modified.

END OF STEPS

**To update BGCF profile**

- 1** Perform the “Add, modify, or delete a BGCF profile procedure” to assign a BGCF Originating Source Info table and a BGCF Default Local Number Routing table. See “[To provision BGCF Profile](#)” (p. 4-142).

END OF STEPS

# To provision BGCF location based routing

## Purpose

This procedure is used to provision BGCF location based routing.

## BGCF location based routing table

A BGCF Location Based Routing table is used to provision routing using the P-Access-Network-Info (PANI) header. The header, along with the P-Asserted-Id is used to provide the location of the calling party.

The BGCF Parameters table is used to define a flag for turning the Location based routing feature on or off. When the Location based routing flag is set to “ON” and the received message has a valid PANI header and other checks have been completed, the BGCF matches the PANI Access-Type and the Access-Info information with the entries defined on the Location Based Routing table screen.

## Before you begin

Observe the following:

- Provision the BGCF PANI Access-Type
- Provision the BGCF PANI Access-Info
- Provision the BGCF Parameters.

## To define BGCF PANI Access-Type

Perform the following at the Provisioning GUI:

1 Select **IMS → IMS Components → BGCF Tables**.

2 Select **BGCF PANI Access-Type**.

3 From the menu, select an **Access-Type ID**.

4 Enter an access standard in the **Access-Type** field.

5 Click **OK**.

END OF STEPS

**To define BGCF PANI Access-Info**

Perform the following at the Provisioning GUI:

- 1 Select **IMS → IMS Components →BGCF Tables**.
- 2 Select **BGCF PANI Access-Info**.
- 3 From the menu, select an **Access-Type ID**.
- 4 Define the type of access in the **Access-Info** field.
- 5 Click **OK**.

**E N D   O F   S T E P S**

**Steps to provision BGCF location based routing table**

Perform the following at the Provisioning GUI:

- 1 Select **IMS → IMS Components → BGCF Tables**.
- 2 In the left pane, expand the **BGCF Location Routing** folder.

| 3 If you want to                                       |  | Then   |
|--|--|--|
| add a BGCF Location Based Routing Table,               |  | Right click <b>BGCF Location Routing</b> and select <b>Add Table</b> from the pull down menu.  |
| modify (= rename) a BGCF Location Based Routing Table, |  | <ol style="list-style-type: none"> <li>1. Select the table you want to modify.</li> <li>2. Right-click and select <b>Rename Table</b></li> <li>3. Modify the name and click <b>OK</b>.</li> </ol> <i>End of procedure.</i> |

| If you want to                              | Then   |
|---|--|
| delete a BGCF Location Based Routing Table, | <ol style="list-style-type: none"> <li>Select the table you want to delete.</li> <li>Right-click and select <b>Delete Table</b>.</li> <li>Click <b>OK</b> to confirm deletion.</li> </ol> <p><i>End of procedure.</i></p> <p><b>Note:</b> BGCF tables can be deleted only when all references to the BGCF table are removed.</p> |

4 Provision the following parameters:

| Parameter                     | Provisioning   |
|-------------------------------|--|
| <b>Called DN Pattern</b>      | Enter the digits of the called party directory number.<br><b>Note:</b> The Called DN Pattern field can contain *, #, x, &, 0-9 and Hex digits. |
| <b>PANI Access-Type</b>       | Type the Access-Type on the BGCF PANI Access-Type screen.  |
| <b>PANI Access-Info</b>       | Type the Access-Info on the BGCF PANI Access-Info screen.  |
| <b>PANI Access-Info Value</b> | Type the Access-Info value for this table in the field.  |
| <b>Target List ID</b>         | Select the target list in this field. This Id will be used to create dynamic next-hop list.  |
| <b>Digit Table Id</b>         | Select the appropriate value of the digit table from the drop-down list.   |

5 Click **OK**.

**Result:** A BGCF Location Based routing table is added.

END OF STEPS

### To activate BGCF location based routing

Perform the following at the Provisioning GUI:

1 Select **IMS → Parameters/timers → BGCF Parameters**.

2 Select **Location Based Routing**.

- 
- 3 From the menu, select a **Calling Party Identity**.
- 

- 4 Click **OK**.

**Result:** BGCF location based routing is activated.

END OF STEPS

---

# To provision BGCF Originating Host ID

## Purpose

This procedure is used to add, modify or delete a BGCF Originating Host ID.

## Before you begin

Observe the following:

- The BGCF Digit Analysis route table must be provisioned before you begin this procedure. Refer to “To provision BGCF DA Route Table” (p. 4-172).

## Steps to provision a BGCF Originating Host ID table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → BGCF Tables**.

**Result:** The **BGCF Tables** window is displayed.

- 2 In the left pane, expand the **BGCF Originating Host ID** folder.

**Result:** The BGCF Originating Host ID tables are listed under the folder in the left pane.

If the folder is empty, add a BGCF Originating Host ID table.

Perform the following steps in the **BGCF Tables** window to add, rename, or delete a BGCF Originating Host ID table :

| If you want to ...                    | then ...  |
|---------------------------------------|---|
| add a BGCF Originating Host ID table, | <ol style="list-style-type: none"><li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li><li>From the <b>Table Number</b> list, select the table number.</li><li>In the <b>Table Name</b> box, type a descriptive table name.</li><li>Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |

| If you want to ...                       | then ...  |
|--|---|
| rename a BGCF Originating Host ID table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>          |
| delete a BGCF Originating Host ID table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a BGCF Originating Host ID table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the BGCF Originating Host ID table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **BGCF Tables** window to add, modify, or delete the BGCF Originating Host ID table attributes:

| If you want to ...                                 | then ...   |
|--|--|
| add the BGCF Originating Host ID table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                                  | then ...  |
|---|---|
| modify a BGCF Originating Host ID table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>BGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a BGCF Originating Host ID table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>               |

**5** Provision the following parameters:

| Parameter                  | Provisioning  |
|----------------------------|---|
| <b>Originating Host ID</b> | Enter the host ID in the <b>Originating Host ID</b> field.<br><br>The host ID can be an IPv4 address, or an IPv6 address, or a domain name with '*' as a wild card. |
| <b>Description</b>         | Enter a brief description in the <b>Description</b> field.  |
| <b>Host Type</b>           | Select the type of the host entered in the <b>Host</b> field, in the <b>Host Type</b> drop-down list.   |
| <b>Subnet Mask</b>         | Enter the appropriate value in the <b>Subnet Mask</b> field, if you have entered an IPv4 or IPv6 address in the <b>Host</b> field.                                  |
| <b>DA Routing Table ID</b> | Select the Digit Analysis routing table ID from the <b>DA Routing Table ID</b> drop-down list.  |

| Parameter                                     | Provisioning  |
|---|---|
| <b>Local Number Routing Table ID</b>          | Select the Local number Digit Analysis table ID from the <b>Local Number Routing Table ID</b> drop-down list.               |
| <b>Location Based Routing Table ID</b>        | Select the Location based routing table ID from the <b>Location Based Routing Table ID</b> drop-down list.                  |
| <b>Enable Routing Based on SDP Media Type</b> | Select the <b>Enable Routing Based on SDP Media Type</b> check box if you want the BGCF to check the SDP media for routing. |

For more information on the parameters, see the topic **BGCF Originating Host Class Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click **OK**.

**Result:** The BGCF Originating Host ID table attributes are provisioned successfully.

END OF STEPS

---

# IBCF provisioning

## Overview

### Purpose

This section provides the procedures that are used to provision the Interconnection Border Control Function (IBCF).

**Note: The IBCF function is not applicable starting ISC Release 21.0. Topics related to IBCF, IBCF Provisioning, and other references to IBCF in this document are only for trial/demonstration purposes.**

### Contents

|                           |       |
|---------------------------|-------|
| To provision IBCF Profile | 4-198 |
|---------------------------|-------|

# To provision IBCF Profile

## Purpose

This topic provides the steps that you have to carry out to provision a profile for an Interconnection Border Control Function (IBCF) service component.

## Related information

In NGSS based services an application component profile is used to define the parameters that are common to one particular instance of a service component, which can run on different IMS servers. When a profile is assigned to a SIPia port, it specifies which configuration is used by the application component that serves this SIPia port. All SIPia ports with the same Generic URI Label (GUL) are identical.

## Before you begin

Observe the following:

- When you create a table, a **table number** is assigned by the system. The number may be changed, but it is recommended to retain the default value.
- The IBCF Profile table supports a maximum of 2048 profiles.
- An IBCF Profile must be assigned to a SIPia port in order to take effect.

## Steps to provision a IBCF Profile table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS > → IMS Components → IBCF Tables**.

**Result:** The **IBCF Tables** window is displayed.

---

- 2 In the left pane, expand the **IBCF Profile** folder.

**Result:** The IBCF Profile tables are listed under the folder in the left pane.

If the folder is empty, add a IBCF Profile table.

Perform the following steps in the **IBCF Tables** window to add, rename, or delete a IBCF Profile table :

| If you want to ...           | then ...  |
|------------------------------|---|
| add a IBCF Profile table,    | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>IBCF Tables</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a IBCF Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>IBCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a IBCF Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a IBCF Profile table, ensure that no table entries are in use.</p> <p><i>End of steps</i></p>  |

**3** Double-click the table to open the list of profiles defined for the table.

Add the IBCF Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **IBCF Tables** window to add, modify, or delete the IBCF Profile table attributes:

| If you want to ...                      | then ...  |
|---|---|
| add the IBCF Profile table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>IBCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a IBCF Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>IBCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a IBCF Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>           |

- 5 Provision the following parameters:

| Parameter                  | Provisioning   |
|----------------------------|--|
| <b>Profile ID</b>          | Choose a <b>Profile ID</b> from the drop-down list.                |
| <b>Profile Description</b> | Enter a brief description in the <b>Profile Description</b> field. |

| Parameter                            | Provisioning   |
|--------------------------------------|--|
| <b>Next Hop URI</b>                  | <p>Enter the next hop URI in the <b>Next Hop URI</b> field.</p> <p>The internal network entity to which the IBCF routes the initial inbound request is derived from this field. If this field is blank, the default I-CSCF in the NGSS parameter profile is used by the IBCF.</p>  |
| <b>Remove Untrusted Headers</b>      | <p>Select <b>Yes</b> in the <b>Remove Untrusted Headers</b> field to remove the headers which should only be exchanged with trusted entities from the SIP messages.</p>  |
| <b>ACR Charging Profile ID</b>       | <p>Select the ACR Charging Profile ID to which the IBCF needs to be mapped in the <b>ACR Charging Profile ID</b> list.</p> <p><b>Note:</b> ACR Charging Profile with ID 0 is regarded as a default profile. The default profile is mapped to 3GPP version 7 ACR messages. The content of default profile is not changeable through the FS GUI. If the IBCF is correlated to default profile and you need to change the version, you can add a new ACR charging profile with the expected version selection and associate the IBCF to the new ACR charging profile.</p> |
| <b>Calling Party Identity Header</b> | <p>Select the Calling Party Identity Header from the <b>Calling Party Identity Header</b> list.</p> <p>This field entry is used only for applying the Network Traffic Management (NTM). The IBCF does not use this field entry for any routing purpose. NTM applies gapping on the originating calling party based on the selected configuration.</p> <p>Alcatel-Lucent recommends retaining the default value.</p> <p><b>Note:</b> NTM is applied at the IBCF, only if a NTM control table is associated with the SIPia port of the IBCF.</p>                         |

| Parameter                                    | Provisioning   |
|--|--|
| <b>SIP Filter Set</b>                        | Select a SIP filter set from the <b>SIP Filter Set</b> drop down list. This SIP filter set will be used to screen the SIP messages that pass through the IBCF from and to the Peer network.  |
| <b>Remote Network IP Version</b>             | Select either <b>IPv4</b> or <b>IPv6</b> in the <b>Remote Network IP Version</b> field to set the IP version of the remote network.  |
| <b>Published Realm</b>                       | Select a realm from the <b>Published Realm</b> drop-down list.<br><br><b>Note:</b> Configuring this field is optional, if <b>Service Based Local Policy Enabled</b> is disabled.   |
| <b>SIP Topology Hiding</b>                   | To enable the IBCF to hide the network topology information in the outbound SIP messages sent to a peer network, select the <b>SIP Topology Hiding</b> check box.<br><br><b>Note:</b> <ul style="list-style-type: none"> <li>The <b>SIP Topology Hiding</b> field can be modified only when the IBCF is out of service.</li> <li>Ensure a valid value is provided in the <b>Topology Hiding Host String</b> field, in the NGSS parameters screen.</li> </ul> |
| <b>Service Based Local Policy Enabled</b>    | If required, enable <b>Service Based Local Policy Enabled</b> by clicking the check box.   |
| <b>Service Based Local Policy Profile ID</b> | Select the <b>Service Based Local Policy Profile ID</b> from the drop-down list if you have enabled <b>Service Based Local Policy Enabled</b> .  |
| <b>SDP Profile ID</b>                        | Select the SDP profile ID that you want to associate with the IBCF Profile in the <b>SDP Profile ID</b> drop-down box.   |
| <b>CANM URI</b>                              | Select the appropriate value from the <b>CANM URI</b> drop down list.<br><br>This field defines the Common Announcement Module URI that is provisioned for a component that needs to send requests to the CANM to play an announcement on behalf of the component.   |

---

For more information on the parameters, see the topic **Ibcf Profile Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

---

- 6 Click OK.

**Result:** The IBCF Profile table attributes are provisioned successfully.

END OF STEPS

---

# E-CSCF provisioning

## Overview

### Purpose

This section provides the procedures that are used to provision the interface to the Emergency CSCF (E-CSCF).

### Contents

|   |                       |
|---|-----------------------|
| <a href="#">Emergency provisioning scenarios</a>              | <a href="#">4-205</a> |
| <a href="#">To provision IMS Emergency Service Identifier</a> | <a href="#">4-208</a> |
| <a href="#">To provision an E-CSCF Profile table</a>          | <a href="#">4-212</a> |

# Emergency provisioning scenarios

## Overview

This topic describes the different Emergency provisioning scenarios:

- E-CSCF provisioning using iFC
- E-CSCF provisioning using ENUM
- E-CSCF provisioning using 3GPP

### Provision the E-CSCF call using iFC

- 1 Provision the E-CSCF profile using one of the ESRM methods:

- VPC-V2
- VPC-V6
- ECSF-HSS
- HSS-VPC-V2

Depending on which ESRM is selected, provision the following:

| ESRM       | Provisioning   |
|------------|--|
| VPC-V2     | Provision all necessary fields in the E-CSCF profile.  |
| VPC-V6     | Provision all necessary fields in the E-CSCF profile.  |
| ECSF-HSS   | <ol style="list-style-type: none"><li>1 Define the Sh interface in the Diameter profile used by the E-CSCF.</li><li>2 Provision all necessary fields in the E-CSCF profile.</li></ol>  |
| HSS-VPC-V2 | <ol style="list-style-type: none"><li>1 Define the Sh interface in the Diameter profile used by the E-CSCF.</li><li>2 Provision all necessary fields in the E-CSCF profile.<br/><i>Note:</i> E-CSCF does not require the FQDN of the next hop for this option.</li></ol> <p>The E-CSCF checks a software license “ESMITCS” first when an initial INVITE is received and the ESRM is HSS-VPC-V2 in its profile. If the license is locked, then the E-CSCF rejects the call.</p> |

Refer to “[To provision an E-CSCF Profile table](#)” (p. 4-212).

- 2 Ensure that the iFC is set so that the E-CSCF can be involved as an AS.

**Provision the E-CSCF call using ENUM**

- 1 Provision the E-CSCF profile using one of the ESRM methods:
  - VPC-V2
  - VPC-V6
  - ECSF-HSS

Depending on which ESRM is selected, provision the following:

| ESRM     | Provisioning  |
|----------|---|
| VPC-V2   | Provision all necessary fields in the E-CSCF profile.   |
| VPC-V6   | Provision all necessary fields in the E-CSCF profile.   |
| ECSF-HSS | <ol style="list-style-type: none"> <li>1. Define the Sh interface in the Diameter profile used by the E-CSCF.</li> <li>2. At a minimum, provision the <b>Next Hop ID</b> and <b>Default Route</b> in the E-CSCF profile.</li> </ol> |

Refer to “[To provision an E-CSCF Profile table](#)” (p. 4-212).

- 2 Ensure that the ENUM database is set up so that the call can be routed to E-CSCF.

**Provision the E-CSCF call using 3GPP**

- 1 Provision the IMS Emergency Identifier List for the E-CSCF profile. Refer to “[To provision IMS Emergency Service Identifier](#)” (p. 4-208).
- 2 Provision 3GPP emergency options in the Emergency Services Parameters of the P-CSCF profile. Refer to “[To provision PCSCF profile](#)” (p. 4-77).
- 3 Provision the E-CSCF profile using one of the ESRM methods:
  - VPC-V2
  - VPC-V6
  - V5-LRF
  - ECSF-HSS
  - SFR-LRF
  - ASSEMBLE-ESRN

Depending on which ESRM is selected, provision the following:

| ESRM          | Provisioning   |
|---------------|--|
| VPC-V2        | Provision all necessary fields in the E-CSCF profile.  |
| VPC-V6        | Provision all necessary fields in the E-CSCF profile.  |
| ECSF-HSS      | <ol style="list-style-type: none"> <li>Define the Sh interface in the Diameter profile used by the E-CSCF.</li> <li>At a minimum, provision the <b>Next Hop ID</b> and <b>Default Route</b> in the E-CSCF profile.</li> </ol>                                  |
| V5-LRF        | Provision all necessary fields in the E-CSCF profile.  |
| SFR-LRF       | <p>Provision all necessary fields in the E-CSCF profile.</p> <p>The E-CSCF checks a software license “ESMITCS” first when an initial INVITE is received and the ESRM is V5-LRF in its profile. If the license is locked, then the E-CSCF rejects the call.</p> |
| ASSEMBLE-ESRN | <ol style="list-style-type: none"> <li>Define the Sh interface in the Diameter profile used by the E-CSCF.</li> <li>At a minimum, provision the Next Hop ID and Default Route in the E-CSCF profile.</li> </ol>  |

Refer to “[To provision an E-CSCF Profile table](#)” (p. 4-212).

# To provision IMS Emergency Service Identifier

## Purpose

This procedure is used to provision an IMS Emergency Service Identifier.

## When you *add* an IMS Emergency Service Identifier table

When you *add* a new IMS Emergency Service Identifier table, the table is empty. You must still add an IMS Emergency Service Identifier.

## Before you begin

Observe the following:

### Frequency

This procedure must be performed whenever an IMS Emergency Service Identifier table must be provisioned.

If the E-CSCF profile is provisioned to support 3GPP and TISPAN standards, use this procedure to provision an IMS Service Identifier table. The IMS Service Identifier table is assigned to the E-CSCF profile.

### Required information

Provisioning data to complete the procedure.

This procedure is performed at the Provisioning GUI.

## Steps to provision a IMS Emergency Service Identifier table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS → IMS Tables**.

**Result:** The **IMS Tables** window is displayed.

- 
- 2 In the left pane, expand the **IMS → General → IMS Emergency Service Identifier** folder.

**Result:** The IMS Emergency Service Identifier tables are listed under the folder in the left pane.

If the folder is empty, add a IMS Emergency Service Identifier table.

Perform the following steps in the **IMS Tables** window to add, rename, or delete a IMS Emergency Service Identifier table :

| If you want to ...                               | then ...   |
|--|--|
| add a IMS Emergency Service Identifier table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>IMS Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a IMS Emergency Service Identifier table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>IMS Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |
| delete a IMS Emergency Service Identifier table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a IMS Emergency Service Identifier table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>                                    |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the IMS Emergency Service Identifier table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **IMS Tables** window to add, modify, or delete the IMS Emergency Service Identifier table attributes:

| If you want to ...  | then ...   |
|---|--|
| add the IMS Emergency Service Identifier table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>IMS Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a IMS Emergency Service Identifier table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>IMS Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a IMS Emergency Service Identifier table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>          |

- 5 Provision the following parameters:

| Parameter                           | Provisioning   |
|-------------------------------------|--|
| <b>Emergency Service Index</b>      | Enter an <b>Emergency Service Index</b> from the menu on this screen.                                  |
| <b>Emergency Service Identifier</b> | In the <b>Emergency Service Identifier</b> field, enter a digit string or URN (uniform resource name). |

---

For more information on the parameters, see the topic **IMS Emergency Service Identifier** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

---

- 6 Click **OK**.

**Result:** The IMS Emergency Service Identifier table attributes are provisioned successfully.

END OF STEPS

---

# To provision an E-CSCF Profile table

## Purpose

This procedure is used to provision a E-CSCF Profile table.

## Steps to provision an E-CSCF Profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → ECSCF Tables**.

**Result:** The **ECSCF Tables** window is displayed.

- 2 In the left pane, expand the **ECSCF Profile** folder.

**Result:** The ECSCF Profile tables are listed under the folder in the left pane.

If the folder is empty, add a E-CSCF Profile table.

Perform the following steps in the **ECSCF Profile** window to add, rename, or delete a E-CSCF Profile table :

| If you want to ...         | then ...  |
|----------------------------|---|
| add a ECSCF Profile table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add ECSCF Profile table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.<br/><i>End of steps</i></li> </ol> |
| rename a E-CSCF table,     | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Rename ECSCF Profile table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.<br/><i>End of steps</i></li> </ol>  |

| If you want to ...     | then ...  |
|------------------------|---|
| delete a E-CSCF table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a E-CSCF profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the E-CSCF profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **ECSCF Profile** window to add, modify, or delete the E-CSCF table attributes:

| If you want to ...                         | then ...  |
|--|---|
| add an E-CSCF profile table attributes,    | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Ecsfc Profile Attributes</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify an E-CSCF profile table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Ecsfc Profile Attributes</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                         | then ...  |
|--|---|
| delete an E-CSCF profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Select the **Routing Methods** tab.

Provision the following parameters:

| Parameter                               | Provisioning  |
|---|---|
| <b>ECSCF Profile Id</b>                 | Select a unique ID for the E-CSCF Profile.<br>This field is associated with an E-CSCF SIPia port and must be defined before an E-CSCF port can be created.  |
| <b>Profile Description</b>              | Type a descriptive name for the E-CSCF Profile.   |
| <b>Emergency Session Routing Method</b> | Select the ESRM value<br>The following fields are enabled if the ESRM is set to “HSS-VPC-v2”. If ESRM is set to another value, the fields are unavailable <ul style="list-style-type: none"> <li>• Support of ESGWRI</li> <li>• Persistent Connection</li> <li>• Heartbeat Timer Interval</li> <li>• HTTP Auth Username</li> <li>• HTTP Auth Password</li> </ul> <b>Note</b> <ol style="list-style-type: none"> <li>Based on the ESRM selected, the emergency call scenario differs.</li> <li>The E-CSCF checks a software license “ESMITCS” first when an initial INVITE is received and the ESRM is HSS-VPC-V2 in its profile. If the license is locked, then the E-CSCF rejects the call.</li> </ol> |

| Parameter   | Provisioning   |
|---|--|
| <b>Next Hop ID</b>                                  | <p>Type the Generic URI Label (GUL) and local domain zone (bgcf-stdn.ecscft.example.com).</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• It is not mandatory to include the BGCF host name as the next hop ID.</li> <li>• In the case of E-CSCF VPC-V6, include the host name of routing proxy.</li> <li>• For the HSS-VPC-V2 ESRM option, the Next Hop ID is not used.</li> <li>• In case of SFR-LRF the Next Hop ID is BGCF URI.</li> <li>• In case of ASSEMBLE-ESRN the Next Hop ID is BGCF URI.</li> </ul>          |
| <b>Default Route</b><br><b>Default Route for V6</b> | <p>Type the default route</p> <p><b>Note</b></p> <p>This default route is used when the following ESRM methods are configured:</p> <ul style="list-style-type: none"> <li>• VPC-V2</li> <li>• ECSF-HSS</li> <li>• V5-LRF</li> <li>• HSS-VPC-V2</li> <li>• SFR-LRF</li> <li>• ASSEMBLE-ESRN</li> </ul> <p>The default route is used for IP mapping when the E-CSCF cannot get an ESRN with UE's IP or SBC domain name. Also, the default Route for V6 is unavailable for all ESRMs.</p>   |
| <b>ACR Charging Profile Id</b>                      | <p>Select the ACR Charging Profile ID to which the E-CSCF needs to be mapped .</p> <p><b>Note</b></p> <p>ACR Charging Profile with ID 0 is regarded as a default profile. The default profile is mapped to 3GPP version 7 ACR messages. The content of default profile is not changeable through the FS GUI. If the E-CSCF is correlated to default profile and you need to change the version, you can add a new ACR charging profile with the expected version selection and associate the E-CSCF to the new ACR charging profile.</p> |

| Parameter                     | Provisioning   |
|-------------------------------|--|
| <b>Extension Delimitation</b> | <p>Type the extension delimitation characters</p> <p><b>Note</b></p> <p>When an emergency call is originated from the 5420 CTS and if the <b>Extension Delimitation</b> field is provisioned, then the E-CSCF removes the corresponding extension number and ensures that the PAID in the outgoing INVITE message is in the correct format.</p> <p>The default value is blank. The maximum allowed characters are 5 and the allowed values are a-z, A-Z and “_”.</p>     |
| <b>HTTP Auth Username</b>     | <p>Enter an appropriate value.</p> <p>This field is used to encode the Authorization header for the HTTP basic authentication.</p>   |
| <b>HTTP Auth Password</b>     | <p>Type the HTTP Auth Password.</p> <p>This field is used to encode the Authorization header for the HTTP basic authentication.</p>  |
| <b>V5 LRF FQDN</b>            | <p>Type the V5 LRF FQDN.</p> <p>This field is available when the ESRM value is <b>V5-LRF</b>, and disabled when the ESRM value is not <b>V5-LRF</b>.</p>   |
| <b>EATF FQDN</b>              | <p>Type the EATF FQDN.</p> <p>This field is provisioned only when emergency VCC is needed.</p> <p><b>Note</b></p> <p>If the option <b>V5-LRF</b> is chosen, all the fields under the <b>VPC Interface</b> group are disabled.</p> <p>The following URI formats are supported for the EATF FQDN and LRF FQDN:</p> <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv4:port</li> <li>• FQDN</li> <li>• FQDN:port</li> <li>• IPv6</li> <li>• IPv6:port</li> </ul> |

| Parameter                            | Provisioning   |
|--------------------------------------|--|
| <b>Prefix to IMEI for SIMless UE</b> | <p>Type the an appropriate value for Prefix to IMEI for SIMless UE.</p> <p>This field is available when the ESRM value is V5-LRF, and cleared when the ESRM value is not V5-LRF. The maximum allowed characters are 7 and the allowed values are “+” and “0” to “9”. “+” must be the first character if it is present.</p>   |
| <b>VPC Interface</b>                 | <p>Type the appropriate VPC FQDN value in the <b>VPC FQDN</b> field.</p> <p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. This field is required when one of the following ESRM methods are configured: <ul style="list-style-type: none"> <li>• VPC-V2</li> <li>• HSS-VPC-V2</li> <li>• SFR-LRF</li> </ul> </li> <li>2. This field is unavailable for IP-Mapping.</li> </ol> |
| <b>VPC Port</b>                      | <p>Type the VPC port number.</p> <p><b>Note</b></p> <p>This field is required when one of the following ESRM methods are configured:</p> <ul style="list-style-type: none"> <li>• VPC-V2</li> <li>• HSS-VPC-V2</li> <li>• SFR-LRF</li> </ul>   |
| <b>VPC Query Timer</b>               | <p>Type the VPC Query Timer.</p> <p><b>Note</b></p> <p>This field is required when one of the following ESRM methods are configured:</p> <ul style="list-style-type: none"> <li>• VPC-V2</li> <li>• HSS-VPC-V2</li> <li>• SFR-LRF</li> </ul>   |
| <b>Source Organization Name</b>      | <p>Type the source organization name field.</p> <p><b>Note</b></p> <p>This field is required when one of the following ESRM methods are configured:</p> <ul style="list-style-type: none"> <li>• VPC-V2</li> <li>• HSS-VPC-V2</li> <li>• SFR-LRF</li> </ul>  |

| Parameter                                | Provisioning   |
|--|--|
| <b>Source Hostname FQDN</b>              | <p>Type the source hostname FQDN.</p> <p><b>Note</b></p> <p>This field is required when one of the following ESRM methods are configured:</p> <ul style="list-style-type: none"> <li>• VPC-V2</li> <li>• HSS-VPC-V2</li> <li>• SFR-LRF (For SFR-LRF this field cannot be left blank).</li> </ul> |
| <b>Source NENA Id</b>                    | <p>Type the source NENA Id.</p> <p><b>Note</b></p> <p>This field is required when one of the following ESRM methods are configured:</p> <ul style="list-style-type: none"> <li>• VPC-V2</li> <li>• HSS-VPC-V2</li> <li>• SFR-LRF</li> </ul>  |
| <b>Source Contact Telephone Number</b>   | <p>Type the source contact telephone number.</p> <p><b>Note</b></p> <p>This field is required when one of the following ESRM methods are configured:</p> <ul style="list-style-type: none"> <li>• VPC-V2</li> <li>• HSS-VPC-V2</li> <li>• SFR-LRF</li> </ul>                                     |
| <b>Certification URI</b>                 | <p>Type the certification URI .</p> <p><b>Note</b></p> <p>This field is required when one of the following ESRM methods are configured:</p> <ul style="list-style-type: none"> <li>• VPC-V2</li> <li>• HSS-VPC-V2</li> <li>• SFR-LRF</li> </ul>  |
| <b>Location in P-Access-Network-Info</b> | <p>Select the location in the PANI.</p> <p>This field is required when VPC-V2 or HSS-VPC-V2 is configured as the ESRM method.</p>  |

| Parameter                       | Provisioning  |
|---------------------------------|---|
| <b>Activate Redundant VPC</b>   | <p>Select the check box to activate the redundant VPC. This check box is enabled only if you select VPC-V2 or HSS-VPC-V2 as the ESRM.</p> <p>Do not enable <b>Active Redundant VPC</b> if SFR-LRF is the ESRM method.</p>   |
| <b>TISPAN/3GPP ECSCF</b>        | <p>Select the check box for the E-CSCF to stay within the Emergency call until the call ends.</p> <p>If the <b>TISPAN/3GPP ECSCF</b> box is checked, assign an Emergency Service Identifier to the profile. Refer to: “<a href="#">To provision IMS Emergency Service Identifier</a>” (p. 4-208)</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• This field must be configured for all ESRM methods. For HSS-VPC-V2 this option is selected by default. For V5-LRF, this option is selected by default and you cannot modify this option.</li> <li>• If ASSEMBLE- ESRN is selected as the ESRM method this flag is checked by default and grayed out.</li> <li>• This field is selected by default for IP mapping. It cannot be changed for IP mapping ESRM.</li> </ul> |
| <b>Reject Non-Emergency URN</b> | <p>Select the check box to reject non-emergency URNs. This option is enabled only if the <b>TISPAN/3GPP ECSCF</b> is selected. If the <b>Reject Non-Emergency URN</b> check box is selected, then Emergency Service Identifiers need to be provisioned. See “<a href="#">To provision IMS Emergency Service Identifier</a>” (p. 4-208).</p>   |
| <b>Support of ESGWRI</b>        | <p>Select the check box. This flag is used to indicate whether or not the ESGWRI should be processed for the NENA v2 interface for the emergency routing information.</p>   |
| <b>Persistent Connection</b>    | <p>Select the check box. This flag is used to indicate whether or not the persistent connection to VPC is activated.</p> <p><b>Note</b></p> <p>If the <b>Persistent Connection</b> field is set to “No”, the <b>Heartbeat Timer Interval</b> field will be grayed out.</p>  |
| <b>Heartbeat Timer Interval</b> | <p>Type the appropriate value in the field. This field is used to indicate how often the heartbeat message should be sent to the VPC.</p>   |

| Parameter               | Provisioning   |
|-------------------------|--|
| Enable SUBSCRIBE/NOTIFY | Select the check box to activate SUBSCRIBE/NOTIFY for the V5-LRF.<br><br>The field is unavailable when ESRM value is not V5-LRF. |

Perform the following steps to provision E-CSCF profile table attributes in the **Miscellaneous** tab:

| Parameter                                       | Provisioning  |
|---|---|
| EAS Response Codes with Final Release Treatment | Click <b>Add</b> in the to add the response codes.<br><br>Select the response code from the list and click <b>Delete</b> to delete the response codes.<br><br><b>Note</b><br>This field must be configured for all ESRM methods.  |
| Emergency Service Identifiers                   | Click <b>Add</b> in the area to add identifiers associated with this profile.<br><br>Select the identifier from the list and click <b>Delete</b> to delete the emergency service identifier.<br><br><b>Note</b><br>Emergency Service Identifiers can be configured only if the <b>Reject Non-Emergency URN</b> check box is selected. |

For more information on the parameters, see the topic **ECSCF Profile Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 6 Click **OK**.

**Result:** The E-CSCF Profile table attributes are provisioned successfully.

END OF STEPS

# NTM provisioning

## Overview

### Purpose

This section provides the procedures that are used to provision the Network Traffic Management (NTM).

### Contents

|                                      |       |
|--------------------------------------|-------|
| To provision an NTM Control table    | 4-222 |
| To provision an NTM Exemption table  | 4-226 |
| To provision an I-CSCF profile table | 4-230 |

# To provision an NTM Control table

## Purpose

This procedure is used to provision an NTM Control table.

## Before you begin

The Provisioning GUI connection must exist.

## Steps to provision an NTM Control table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → NTM Tables**.

**Result:** The **NTM Tables** window is displayed.

- 2 In the left pane, expand the **NTM Control Table** folder.

**Result:** The NTM Control tables are listed under the folder in the left pane.

If the folder is empty, add an NTM Control table.

Perform the following steps in the **NTM Tables** window to add, rename, or delete an NTM Control Table table :

| If you want to ...        | then ...   |
|---------------------------|--|
| add an NTM Control table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add Control Table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...           | then ...  |
|------------------------------|---|
| rename an NTM Control table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename Control Table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete an NTM Control table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an NTM Control table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>             |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the NTM Control table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **NTM Tables** window to add, modify, or delete the NTM Control table attributes:

| If you want to ...                    | then ...  |
|---------------------------------------|---|
| add the NTM Control table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>NTM Controls</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                      | then ...   |
|---|--|
| modify an NTM Control table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>NTM Controls</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete an NTM Control table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                |

## 5 Provision the following parameters:

| Parameter          | Provisioning                                     |
|--------------------|--|
| <b>Start (UTC)</b> | Specify the start date and time for NTM Control. |
| <b>End (UTC)</b>   | Specify the end date and time for NTM Control    |

| Matching Criteria Parameters | Provisioning                                    |
|------------------------------|---|
| <b>Request Method</b>        | Unique Id for a control in an NTM Control Table |
| <b>Match On</b>              | Select Destination or Origination               |
| <b>Match Type</b>            | Type of Matching String                         |
| <b>Port</b>                  | Port Number                                     |
| <b>IP Address Type</b>       | IP Address Type IPV4 or IPV6                    |
| <b>Netmask</b>               | IP Address Masking                              |

| Matching Criteria Parameters | Provisioning                                      |
|------------------------------|---|
| <b>Phone Context Type</b>    | Phone Context Type ( Domain or Global Digits)     |
| <b>Phone Context</b>         | Phone Context String                              |
| <b>Matching String</b>       | Contain Full or portion of the SIP URI or Tel URI |

| Control Parameters              | Provisioning  |
|---------------------------------|---|
| <b>Map Mechanism</b>            | Type of Code Control  |
| <b>Gapping Mechanism</b>        | Type of Call Gapping Mechanism  |
| <b>Gap Interval (milli sec)</b> | Interval of time in which call gapping takes place. 0 means allow all calls. -1 means block all calls |
| <b>Blocked Percentage</b>       | % of traffic blocked during the specified duration  |

| Treatment Parameters             | Provisioning   |
|----------------------------------|--|
| <b>Treatment Mechanism</b>       | Type of Error Response   |
| <b>SIP Error Code</b>            | SIP Error response Code  |
| <b>Reason Cause Code</b>         | Valid Cause Code defined in ITU Q.850  |
| <b>Reason Text</b>               | Text for Reason Header   |
| <b>Announcement Treatment ID</b> | When the Treatment Mechanism is Announcement, then the Announcement Treatment ID must be non-zero. Range 0 - 10. |

For more information on the parameters, see the topic **IMS - NTM Tables** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 6 Click OK.

**Result:** The NTM Control table attributes are provisioned successfully.

END OF STEPS

# To provision an NTM Exemption table

## Purpose

This procedure is used to provision an NTM Exemption table.

## Before you begin

The Provisioning GUI connection must exist.

## Steps to provision an NTM Exemption table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → NTM Tables**.

**Result:** The **NTM Tables** window is displayed.

- 2 In the left pane, expand the **NTM Exemption Table** folder.

**Result:** The NTM Exemption tables are listed under the folder in the left pane.

If the folder is empty, add an NTM Exemption table.

Perform the following steps in the **NTM Tables** window to add, rename, or delete an NTM Exemption table:

| If you want to ...          | then ...  |
|-----------------------------|---|
| add an NTM Exemption table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add NTM Exemption Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...             | then ...   |
|--------------------------------|--|
| rename an NTM Exemption table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename NTM Exemption Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete an NTM Exemption table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a NTM Exemption table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>                   |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the NTM Exemption table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **NTM Tables** window to add, modify, or delete the NTM Exemption table attributes:

| If you want to ...                      | then ...  |
|---|---|
| add the NTM Exemption table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>NTM Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                         | then ...  |
|--|---|
| modify the NTM Exemption table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>NTM Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol> |
| delete the NTM Exemption table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.<br/><i>End of steps.</i></li> </ol>              |

**5** Provision the following parameters:

| Matching Criteria Parameter | Provisioning  |
|-----------------------------|---|
| <b>Request Method</b>       | SIP Request Methods                                 |
| <b>Match On</b>             | Match the control on the Origination or Destination |
| <b>Match Type</b>           | Type of Matching String                             |
| <b>Port</b>                 | Port Number   |
| <b>IP Address Type</b>      | IP Address Type IPV4 or IPV6                        |
| <b>Netmask</b>              | IP Address Masking                                  |
| <b>Phone Context Type</b>   | Phone Context Type ( Domain or Global Digits)       |
| <b>Phone Context</b>        | Phone Context String                                |
| <b>Matching String</b>      | Contain Full or portion of the SIP URI or Tel URI   |

| Control Parameter        | Provisioning                    |
|--------------------------|---------------------------------|
| Map Mechanism            | Select an option from the list. |
| Gapping Mechanism        | Select an option from the list. |
| Gap Interval (milli sec) | Enter a value                   |
| Blocked Percentage       | Enter a value                   |

| Treatment Parameters      | Provisioning                    |
|---------------------------|---------------------------------|
| Treatment Mechanism       | Select an option from the list. |
| Sip Error Code            | Select an option from the list. |
| Reason Cause Code         | Enter a value                   |
| Reason Text               | Type the string.                |
| Announcement Treatment ID | Enter a value                   |

For more information on the parameters, see the topic **NTM Exemption** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 6 Click **OK**.

**Result:** The NTM Exemption table attributes are provisioned successfully.

END OF STEPS

# To provision an I-CSCF profile table

## Purpose

This procedure is used to provision an I-CSCF profile table.

## Steps to provision an I-CSCF profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **ICSCF Tables**.

**Result:** The **ICSCF Tables** window is displayed.

- 2 In the left pane, expand the **ICSCF Profile** folder.

**Result:** The ICSCF Profile tables are listed under the folder in the left pane.

If the folder is empty, add an ICSCF Profile table.

Perform the following steps in the **ICSCF Tables** window to add, rename, or delete an ICSCF Profile table :

| If you want to ...             | then ...   |
|--------------------------------|--|
| add an ICSCF Profile table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>ICSCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename an ICSCF Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>ICSCF Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |

| If you want to ...            | then ...   |
|-------------------------------|--|
| delete a ICSCF Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a ICSCF Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the ICSCF Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **ICSCF Tables** window to add, modify, or delete the ICSCF Profile table attributes:

| If you want to ...                         | then ...  |
|--|---|
| add the ICSCF Profile table attributes,    | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>ICSCF Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify the ICSCF Profile table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>ICSCF Tables</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                         | then ...  |
|--|---|
| delete the ICSCF Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter                  | Provisioning  |
|----------------------------|---|
| <b>Profile Id</b>          | Defines the Interrogating Call Session Control Function (I-CSCF) profile identifier.<br>Enter a unique Profile ID.  |
| <b>Profile Description</b> | Description of the type of call requests that are processed by this I-CSCF profile.<br>Type a name for the profile.   |
| <b>Max S-CSCF Retry</b>    | Defines how many times an I-CSCF should try to select a S-CSCF for initial registration.<br>Enter a value.  |
| <b>S-CSCF URI</b>          | Default S-CSCF name, which is used by I-CSCF, if HSS does not return a S-CSCF name nor S-CSCF capabilities in LIA response.<br>Type an URI.<br><b>Note:</b> To use the P-NAPTR functionality, besides the P-NAPTR tables, specify the SCSF name. Use the Generic URI Label (GUL) and home domain (scsf-stdn.example.com) instead of the GUL and local zone domain (scsf-stdn.east.example.com). This is used to find a match in the P-NAPTR database. The P-NAPTR database returns the S-CSCFs to try which S-CSCF includes the local zone domains in the FQDN. |

| Parameter                                    | Provisioning  |
|--|---|
| <b>BGCF URI</b>                              | BGCF domain name. Points to the default BGCF Host URI, unless specified here for I-CSCF.<br><br>Type an URI.  |
| <b>PSI Subdomain List ID</b>                 | Character from 1 to 5 identifying a predefined subdomain list.<br><br>Select a value from the list.   |
| <b>Register Without Authorization Header</b> | This option defines the action to taken when the received REGISTER message does not have a private user identity in the authorization header.<br><br>Select a value form the list.  |
| <b>Originating Host List Index</b>           | Points to the “Originating Hosts” table, which is used by the I-CSCF for post route selection, “class” population.<br><br>Select a value form the list.   |
| <b>ENUM Profile Index</b>                    | This ENUM Profile ID points to the ENUM profile. These ENUM profile options allow the operator to control aspects of whether and how the ICSCF makes ENUM queries.<br><br>Select a value form the list.   |
| <b>Address Resolution Method</b>             | Specifies the method that will be used by the I-CSCF for resolving destination addresses for routing purposes<br><br>Select a value form the list.  |
| <b>Change SIP URI To Tel URI</b>             | For a termination request, if the Request-URI includes a SIP URI contains a E.164 number in the user part and a “user=phone” parameter, the I-CSCF will replace the Request-URI with a Tel URI, if this parameter is set to “Yes”.<br><br>Select the check-box to enable. |

| Parameter                                 | Provisioning  |
|---|---|
| <b>Enforce Phone-Context When Routing</b> | <p>Provides the option to enforce the presence of the phone-context parameter when deciding whether to route a SIP request that has local telephone number (ie: not an E.164 global number). The phone-context parameter is intended to provide further information for local numbers.</p> <p>Select the check-box to enable.</p>   |
| <b>Additional Cx Query</b>                | <p>Decides if an additional Cx query is needed after the Cx and the ENUM query.</p> <p>Select the ratio button.</p>   |
| <b>Post Route Selection</b>               | <p>When the value of this field is set to "Yes", the I-CSCF will perform Post Route Selection, e.g., static rules based on originating host after ENUM query.</p> <p>Select the ratio button.</p>   |
| <b>Route Based on CgPN</b>                | <p>This option allows an operator to configure the ICSCF to support routing based on the calling party (CgPN).</p> <p>Select the ratio button.</p>  |
| <b>ACR Charging Profile Id</b>            | <p>IMS ACR Charging Profile ID</p> <p>Select a value from the list.</p> <p><b>Note:</b> ACR Charging Profile with ID 0 is regarded as a default profile. The default profile is mapped to 3GPP version 5 ACR messages. The content of default profile is not changeable through the FS GUI. If the I-CSCF is correlated to default profile and you need to change the version, you can add a new ACR charging profile with the expected version selection and associate the I-CSCF to the new ACR charging profile.</p> |
| <b>Apply NTM Prior to ENUM</b>            | <p>When this parameter is set to 'No', NTM Control Codes are compared with the R-URI in its final format. If it is set to 'Yes', the NTM Control Codes are compared with the received R-URI after the SIP to Tel URI Conversion.</p> <p>Select the check-box to enable.</p>   |

| Parameter  | Provisioning   |
|--|--|
| Action For Redirection Responses                   | Action for 301/302/305 redirection responses(0 = Proxy(default) , 1 = Evaluate-Route, 2 = Route-Direct<br>Select a value form the list.  |
| Use Configured Home Domain In R-URI                | Use Configured Home Domain in R-URI.Indicates whether I-CSCF will change the R-URI for single domain support.The default will be existing behavior,if the flag is turned on then I-CSCF will not change the R-URI.<br>Select the check-box to enable.  |
| Route To BGCF For Enum Timeout                     | Route to BGCF for ENUM Timeout.<br>Select the ratio button.  |
| CANM URI   | Common Announcement Module URI that may be provisioned for a component that needs to send requests to the CANM to play an announcement on behalf of the component.<br>Select a value form the list.  |
| Support PServed- User Header                       | This option controls whether I-CSCF supports P-Served-User header, specifically, whether I-CSCF can do Cx or ENUM query based on PUID from P-Served- User header, and whether I-CSCF pass this header to S-CSCF.<br>Select the check-box to enable.  |
| Response Code for De-Registration to Remote S-CSCF | This option specifies the response code the I-CSCF shall return for De-Registration requests destined to a remote S-CSCF. This field shall only apply if the NGSS parameter UERe-Registration for Geo-Redundancy is enabled. If the UE Re-Registration for Geo-Redundancy field is disabled, this field should be grayed out.<br>Select a value form the list. |
| SIP Error Treatment Table                          | SIP Error Treatment Table ID referred by this profile.<br>Select a value form the list.  |

| Parameter      | Provisioning  |
|----------------|---|
| Sip Filter Set | This field identifies the filter set that this instance uses for SIP message screening. A value of 0(zero) specifies that SIP message screening is not configured at this instance. A non-zero value within the defined range is an index to a record in the SIP Filter Set table.<br><br>Select a value from the list. |

For more information on the parameters, see the topic **Icscf Profile Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The ICSCF Profile table attributes are provisioned successfully.

END OF STEPS

---

# EEAS provisioning

## Overview

### Purpose

This section provides the procedures that are used to provision the interface to the E.164 Expansion Application Server (EEAS).

The EEAS is used on the IMS network when number normalization has to be performed for the telephone numbers that are dialed by IMS subscribers.

### Contents

|  |       |
|--|-------|
| To provision an E.164 Expansion AS profile | 4-238 |
|--|-------|

# To provision an E.164 Expansion AS profile

## Purpose

This procedure is used to provision an IMS EEAS profile.

## Steps to provision a EEAS profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Tables**.

**Result:** The **IMS Tables** window is displayed.

- 2 In the left pane, expand the **Dual Mode Subscriber (DMS)** folder and then the **EEAS** folder.

**Result:** The EEAS tables are listed under the folder in the left pane.

If the folder is empty, add a EEAS table.

Perform the following steps in the **IMS Tables** window to add, rename, or delete a EEAS table :

| If you want to ...   | then ...  |
|----------------------|---|
| add a EEAS table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add EEAS table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a EEAS table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Rename EEAS table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |

| If you want to ...   | then ...  |
|----------------------|---|
| delete a EEAS table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a EEAS table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the EEAS table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **IMS Tables** window to add, modify, or delete the EEAS table attributes:

| If you want to ...              | then ...  |
|---------------------------------|---|
| add the EEAS table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>EEAS</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a EEAS table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>EEAS</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...              | then ...  |
|---------------------------------|---|
| delete a EEAS table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter                 | Provisioning   |
|---------------------------|--|
| <b>Lower Bound Digits</b> | Type the lower-bound number of digits to consider for expansion.   |
| <b>Prefix to Prepend</b>  | <p>Type the digits that are added in front of the called number.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>This step applies only for IMS terminating sessions</li> <li>The Profile Id field is associated with an EEAS SIPia port and must be defined before an EEAS port can be created.</li> </ul> |

For more information on the parameters, see the topic **EEAS Profile** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

6 Click **OK**.

**Result:** The EEAS table attributes are provisioned successfully.

END OF STEPS

# IMS gateway function provisioning

## Overview

### Purpose

This section describes the provisioning of the IMS gateway.

### Contents

|   |       |
|---|-------|
| To provision Online Charging Trigger Data table | 4-242 |
| To provision MRF Announcement Interface profile | 4-245 |
| To provision MRF Announcement Data table        | 4-247 |
| To provision IGWF profile                       | 4-250 |

# To provision Online Charging Trigger Data table

## Purpose

This procedure is used to add, modify, or delete Online Charging Trigger Data table. An Online Charging Data table defines triggers for online charging conditions.

## Before you *delete* a table

Before you *delete* a table, delete all records.

## Steps to provision Online Charging Data table

Perform the following at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **IGWF Tables**.
- 2 In the left pane, expand the **Online Charging Trigger Data** folder.
- 3

| If you want to ... | then ...  |
|--------------------|---|
| add a table,       | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add Online Charging Trigger Data table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.<br/><i>End of steps</i></li> </ol> |
| modify a table,    | Select the table you want to rename, then select <b>Rename Table</b> from the menu. Rename the table and click OK.<br><i>End of steps</i>   |
| delete a table,    | <ol style="list-style-type: none"> <li>1. Select the table you want to delete,</li> <li>2. Select <b>Delete Table</b> from the menu</li> <li>3. Click <b>Yes</b><br/><i>End of steps</i></li> </ol>   |

**4** Click **OK**.

**Result:** The **Online Charging Trigger Data** table is added or modified. The table automatically populates with a set of trigger IDs.

**5** Select **IMS → IMS Components → IGWF Table**.

**6** Double-click on the specific table.

| If you want to ... | Then  |
|--------------------|---|
| add attributes,    | Right-click and select <b>Add Table Attributes</b> .  |
| modify attributes, | Right-click and select <b>Modify Table Attributes</b> .   |
| delete attributes, | <ol style="list-style-type: none"> <li>1. Select the profile you want to delete.</li> <li>2. Right-click and select <b>Delete Table Attributes</b>.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of procedure.</i></p> <p><b>Result:</b> The attributes are deleted.</p> |

**7** Provision the following parameters in the **Online Charging Trigger Data Attributes** window:

| Parameter                    | Provisioning   |
|------------------------------|--|
| <b>Trigger Id</b>            | This field is the identifier for the online charging trigger.  |
| <b>Condition Description</b> | This field describes conditions that can occur during online charging.   |
| <b>Reason Text</b>           | <p>This field defines the text string to return to the UE in the SIP Reason header when the trigger condition is met.</p> <p><b>Additional Information:</b></p> <p>For descriptions of the attributes, see <i>Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual</i>, 275-900-379.</p> |

**8** Click **OK**.

**Result:** The attributes are added or updated.

END OF STEPS

# To provision MRF Announcement Interface profile

## Purpose

This procedure is used to add, modify, or delete an MRF Announcement Interface profile.

## Before you add an MRF Announcement Interface profile

Before you add a table, ensure that an MRF Announcement Data table is provisioned.

## Before you delete an MRF Announcement Interface profile

Before you *delete* a table, ensure that the profile is not used by an IGWF profile.

## Steps to provision MRF Announcement Interface profile table

Perform the following at the Provisioning GUI:

1 Select **IMS → Global Tables**.

2 In the left pane, expand the **MRF Ann Interface Profile** folder.

| 3 | If you want to ... | then ...   |
|---|--------------------|--|
|   | add a table,       | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add MRF Ann Interface Profile</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <i>End of steps</i> |
|   | modify a table,    | Select the table you want to rename, then select <b>Rename Table</b> from the menu. Rename the table and click OK.<br><i>End of steps</i>  |
|   | delete a table,    | <ol style="list-style-type: none"><li>1. Select the profile you want to delete,</li><li>2. Select <b>Delete Table</b> from the menu</li><li>3. Click <b>Yes</b></li></ol> <i>End of steps</i>  |

4 Click **OK**.

**Result:** An MRF Ann Interface Profile is added.

- 
- 5 Select **IMS → Global Tables**.

---

  - 6 In the left pane, expand the **MRF Ann Interface Profile** table group.

---

  - 7 Double-click on the specific MRF Ann Interface Profile table.

| If you want to ... | Then  |
|--------------------|---|
| add attributes,    | <ol style="list-style-type: none"> <li>1. Right-click on the desired entry and select <b>Add Table Attributes</b>.</li> <li>2. Configure values for the attributes.</li> </ol> <p><i>End of steps</i></p>   |
| modify attributes, | <ol style="list-style-type: none"> <li>1. Select the profile you want to modify</li> <li>2. Right-click and select <b>Modify Table Attributes</b>.</li> <li>3. Modify the values for the attributes.</li> </ol> <p><i>End of steps</i></p>                              |
| delete attributes  | <ol style="list-style-type: none"> <li>1. Select the profile you want to delete</li> <li>2. Right-click and select <b>Delete Table Attributes</b>.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> <p><b>Result:</b> The attributes are deleted.</p> |

**Additional information:** For descriptions of the attributes, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

- 
- 8 Click **OK**.
- Result:** The attributes are added or updated.

END OF STEPS

---

# To provision MRF Announcement Data table

## Purpose

This topic describes how to add, modify, or delete an MRF Announcement Data table and how to import and export table attributes. The table is used to define announcement that are played for online charging events.

**Important!** The user cannot modify a table or add, modify, or delete individual table attributes.

To modify the table or table attributes, delete the table, add a new table, and import a new table.

## Table format

The table attributes are imported and exported in a comma-separated file format (CSV).

**Important!** The *TableType=28673* is required and must not be changed.

The following lines are an example of a CSV file that can be imported:

```
TableType=28673 Ann ID,Ann Description,Ann Filename 1, Description for
ann 1, file/path/annc_1.wav, 2, Description for annc 2, file/
path/annc_2.wav, 3, Description for annc 3, file/path/annc_3.wav,
```

## Before you begin

On the MRF, ensure that the audio files for the announcements are available under the path that you defined in **Ann Filename**.

## Table procedure

Perform the following steps at the Provisioning GUI:

- 1 Select **System Admin → Announcement/Treatment Table**.
  
- 2 In the left pane, expand the **MRF Announcement Data Tables** folder.

| 3 | If you want to ... | then ...   |
|---|--------------------|--|
|   | add a table,       | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The Add MRF Announcement Data Tables window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><b>Result:</b><br/>An MRF Announcement Data table is added.</p> <p><i>End of steps</i></p> |
|   | delete a table,    | <ol style="list-style-type: none"> <li>1. Select the table you want to delete.</li> <li>2. Click the <b>Delete</b> button on your keyboard.</li> <li>3. Click <b>Yes</b>.</li> </ol> <p><i>End of steps</i></p>  |

END OF STEPS

## Steps to Import and export table attributes

A table import only adds new attributes that are in the table you import. When you import a table, existing table attributes are not overwritten or deleted.

Perform the following steps at the Provisioning GUI:

- 1 Select **System Admin** → **Announcement/Treatment Table**.
- .....
- 2 In the left pane, expand the **MRF Announcement Data Tables** folder to expand this folder.
- .....
- 3 Select the MRF Announcement Data Table, right-click, and select **Open**.

4

| If you want to ... | then ...   |
|--------------------|--|
| import a table,    | <ol style="list-style-type: none"><li>1. Right-click and select <b>Import Table</b></li><li>2. In the Browse window, select a path and filename and click <b>Open</b>.</li></ol> <p><i>End of steps</i></p>                    |
| export a table,    | <ol style="list-style-type: none"><li>1. Right-click and select <b>Export Table</b></li><li>2. In the Browse window, select a path and filename to store the table and click <b>Save</b>.</li></ol> <p><i>End of steps</i></p> |

END OF STEPS

# To provision IGWF profile

## Purpose

This procedure is used to add, modify, or delete an IGWF profile.

## Before you **delete** an IGWF profile

Before you *delete* a table, ensure that the profile is not used by a SIPia port.

## IGWF profile table procedure

Perform the following at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **IGWF Tables**.

- 2 In the left pane, expand the **IGWF Profile** folder.

3

| If you want to ... | then ...   |
|--------------------|--|
| add a table,       | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/> <b>Result:</b> The <b>Add IGWF Profile</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.<br/> <b>Result:</b><br/> An IGWF Profile is added.<br/> <i>End of steps</i></li> </ol> |
| modify a table,    | Select the table you want to rename, then select <b>Rename Table</b> from the menu. Rename the table and click OK.<br><br><i>End of steps</i>  |
| delete a table,    | <ol style="list-style-type: none"> <li>Select the profile you want to delete,</li> <li>Select <b>Delete Table</b> from the menu</li> <li>Click <b>Yes</b><br/> <i>End of steps</i></li> </ol>  |

4 Select IMS → IMS Components → IGWF Tables Right-click on the IGWF Profile table.

| If you want to ... | Then   |
|--------------------|--|
| add attributes,    | <ol style="list-style-type: none"><li>1. Select <b>Add Table Attributes</b>.</li><li>2. Configure values for the attributes.</li><li>3. Click <b>OK</b>.</li></ol> <p><b>Result:</b><br/>The attributes are added.<br/><i>End of steps</i></p> |
| modify attributes, | <ol style="list-style-type: none"><li>1. Select <b>Modify Table Attributes</b>.</li><li>2. Modify the values for the attributes.</li><li>3. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p>  |
| delete attributes  | <ol style="list-style-type: none"><li>1. Select <b>Delete Table Attributes</b>.</li><li>2. Click <b>OK</b>.</li></ol> <p><i>End of steps</i><br/><b>Result:</b> The attributes are deleted.</p>  |

**Additional information** For descriptions of the attributes, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS.....

# P-NAPTR provisioning

## Overview

### Purpose

This section provides the tasks that are required to provision the pseudo naming authority pointer (P-NAPTR ) records.

P-NAPTR records allow a system to know about the other system locations (for the purpose of providing element geo-redundancy), without the need for an actual NAPTR DNS server. P-NAPTR records are office based provisioning, available to any NGSS .

Besides the configuration changes below also the I-CSCF profile, S-CSCF Profile, E-CSCF profile, BGCF target URI and NGSS Parameter and timers. Refer to these sections for more information.

### Contents

|   |                       |
|---|-----------------------|
| <a href="#">To provision a P-NAPTR Region</a>     | <a href="#">4-253</a> |
| <a href="#">To provision a P-NAPTR Target URI</a> | <a href="#">4-257</a> |

# To provision a P-NAPTR Region

## Purpose

This procedure is used to provision a pseudo naming authority pointer (P-NAPTR) Regions.

## Description

The P-NAPTR Region fully-qualified domain name (FQDN) needs to be populated using the Generic URI Label (GUL) and the home domain of the specific components that P-NAPTR lookups are done. Currently, those components include the BGCF, I-SCSF, S-SCSF, and E-CSCF. Each Region FQDN will have P-NAPTR target URI's associated with them and are used to assign a preferred or alternate tag and weight field to the specific target URI's.

Note that if more than one external emergency host URI is needed when provisioning the P-CSCF to route emergency calls, the Pseudo-NAPTR record must be provisioned. This record will be used by the Emergency Host URI in the P-CSCF profile to support emergency call sessions.

## Before you begin

Points to remember:

### Required information

**Important!** Before provisioning **P-NAPTR Region** tables **P-NAPTR Target URI** tables must have been provisioned prior.

## Steps to provision a P-NAPTR Region

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS General Tables**.

- 2 In the left pane, expand the **P-NAPTR Region** folder to display the tables. If the folder is empty, add a table.

| 3 | If you want to ...                  | then ...   |
|---|-------------------------------------|--|
|   | Add P-NAPTR Region attributes,      | <ol style="list-style-type: none"> <li>Select the <b>P-NAPTR Region</b> and click <b>Open</b> in the Tables menu or double click <b>P-NAPTR Region</b> to open the <b>P-NAPTR Region</b> table.</li> <li>Select an empty row in the table and click <b>Add Table Attribute</b> from the Tables menu to display the <b>P-NAPTR Region</b> window.</li> <li>Proceed with <a href="#">Step 4</a></li> </ol>   |
|   | Modify P-NAPTR Region attributes,   | <ol style="list-style-type: none"> <li>Select the <b>P-NAPTR Region</b> and click <b>Open</b> in the Tables menu or double click <b>P-NAPTR Region</b> to open the <b>P-NAPTR Region</b> table.</li> <li>Select the row you want to modify and click <b>Modify Table Attribute</b> from the Tables menu to display the <b>P-NAPTR Region</b> window.</li> <li>Proceed with <a href="#">Step 4</a></li> </ol>   |
|   | Delete a P-NAPTR Region attributes, | <p>Note: Before you <i>delete</i> a P-NAPTR Region table, you must make sure that all related records have been deleted.</p> <ol style="list-style-type: none"> <li>Select the <b>P-NAPTR Region</b> table you want to delete, then select <b>Delete Table</b> from the Tables menu. The following message is displayed:<br/><i>Please delete all the records of this table prior to delete</i></li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of procedure.</i></p> |

#### 4 Provision the following parameters:

| Parameter                  | Description   |
|----------------------------|---|
| <b>P-NAPTR Region ID</b>   | Select an ID number from the <b>P-NAPTR Region ID</b> drop-down list.   |
| <b>P-NAPTR Region FQDN</b> | <p>Define the <b>P-NAPTR Region FQDN</b>.</p> <p>Note: Whenever a P-NAPTR Region FQDN is entered, the input will be translated into lowercase characters.</p> <p>Maximum of 255 characters are allowed.</p> |

| Parameter                              | Description  |
|--|--|
| <b>P-NAPTR group affinity</b>          | <p>The <b>P-NAPTR group affinity</b> parameter is used to specify the maximum number of pNATPR records in a pNAPTR group to be tried.</p> <p>Select the value from the <b>P-NAPTR Group Affinity</b> drop-down list. When this value is specified, it overwrites the per-switch value provisioned in the NGSS Parameter window.</p> <p>When set to “ALL”, all records in the per-region pNAPTR group are tried before moving to the next group.</p> <p>When set to “None”, it indicates that the per-region value is not provisioned and the per-switch value is used.</p> |
| <b>SIP Next Hop Limit</b>              | <p>The <b>SIP Next Hop Limit</b> parameter is used to specify the per-region SIP next hop limit.</p> <p>Select the value from the <b>SIP Next Hop Limit</b> drop-down list. When this value is specified, it overwrites the per-switch value provisioned in the NGSS Parameter window.</p> <p>When set to “None”, the existing per-switch SIP next hop limit is used.</p>  |
| <b>SIP Alternate Route for SIP 503</b> | <p>The <b>SIP Alternate Route for SIP 503</b> parameter is used to specify the per-region alternate SIP route for SIP 503.</p> <p>Select a value from the <b>SIP Alternate Route for SIP 503</b> drop-down list. When this value is specified, it overwrites the per-switch value provisioned in the NGSS Parameter window.</p> <p>When set to “None”, the existing per-switch value of alternate route for SIP 503 is used.</p>   |

| Parameter                  | Description  |
|----------------------------|--|
| <b>P-NAPTR Record List</b> | <p>Use the area <b>P-NAPTR Record List</b> to add/modify/delete a P-NAPTR URI Record.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• To specify the transport protocol to be used with the pNATPR RR, set the <b>Service Type</b> parameter in the <b>P-NAPTR URI Record</b> window.</li> <li>• If P-NAPTR RR has a service type=TLS but TLS is not supported on Mw, then the P-NAPTR RR with service type=TLS will be discarded.</li> <li>• If original URI is SIPS URI and TLS transport is used on Mw then any service type field of P-NAPTR RR will be ignored.</li> </ul> |

**5** Click **OK**.

For more information on the parameter description, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision a P-NAPTR Target URI

## Purpose

This procedure is used to add, modify or delete a pseudo naming authority pointer (P-NAPTR) Target URI.

## Description

P-NAPTR records allow a system to know about the other system locations (for the purpose of providing element geo-redundancy), without the need for an actual NAPTR DNS server.

The P-NAPTR Target URI table is used for all the URI's that will be used to try and reach primary and alternate locations. These URI's are then used in the P-NAPTR Region table when attempting to reach primary and alternate locations.

Note that these resolvable URI's include the local zone domain of the regions you are attempting to reach. When used for routing, they will return a set of IP's that will be used to route the request.

Also, note that if more than one external emergency host URI is needed when provisioning the P-CSCF to route emergency calls, the Pseudo-NAPTR record must be provisioned. This record will be used by the Emergency Host URI in the P-CSCF profile to support emergency call sessions.

## Before you begin

Points to remember:

### Required information

Verification should be done to make sure that the URI's added to the P-NAPTR table can be resolved by DNS before populating the table with these names.

HSS data needs to be set up to return a server capability for the subscribers. The server capability should be in the format *scsf-stdn.homedomain* to be able to find a match after a P-NAPTR lookup. When using the server capability for finding an Emergency Application Server for E911 calls, the EAS needs to be provisioned in the HSS server capability as *IEAS-STDN.HOMEDOMAIN* in order for P-NAPTR lookup to find a match when routing to an EAS.

HSS data should be set up to allow the UE's to roam to all the possible visited networks identified in the P-NAPTR Target URI table. For example, if our choices for finding an S-CSCF for the request are *scsf-stdn.west.ims.name.com*, *scsf-stdn.east.ims.name.com* and *scsf-stdn.central.ims.name.com*, then HSS needs to be setup to allow all the possible visited regions (ie.. *east.ims.name.com*, *west.ims.name.com* *central.ims.name.com*) that the UE could end up being registered with.

**Steps to provision a P-NAPTR Target URI table**

Perform the following steps at the Provisioning GUI:

**1** Select **IMS → IMS General Tables**.

**2** In the left pane, expand the **P-NAPTR Target URI** folder to display the tables. If the folder is empty, add a table.

| <b>3</b> | <b>If you want to ...</b>                     | <b>then ...</b>  |
|----------|---|--|
|          | Add P-NAPTR Target URI table attributes,      | <ol style="list-style-type: none"> <li>Select the <b>P-NAPTR Target URI</b> and click <b>Open</b> in the Tables menu or double click <b>P-NAPTR Target URI</b> to open the <b>P-NAPTR Target URI</b> table.</li> <li>Select an empty row in the table and click <b>Add Table Attribute</b> from the Tables menu to display the <b>P-NAPTR Target URI</b> screen.</li> <li>Proceed with <a href="#">Step 4</a></li> </ol>     |
|          | Modify P-NAPTR Target URI table attribute,    | <ol style="list-style-type: none"> <li>Select the <b>P-NAPTR Target URI</b> and click <b>Open</b> in the Tables menu or double click <b>P-NAPTR Target URI</b> to open the <b>P-NAPTR Target URI</b> table.</li> <li>Select the row you want to modify and click <b>Modify Table Attribute</b> from the Tables menu to display the <b>P-NAPTR Target URI</b> screen.</li> <li>Proceed with <a href="#">Step 4</a></li> </ol> |
|          | Delete a P-NAPTR Target URI table attributes, | <p>Note: Before you <i>delete</i> a P-NAPTR Target URI table attribute , you must make sure that all related records have been deleted from the P-NAPTR Region.</p> <ol style="list-style-type: none"> <li>Select the <b>P-NAPTR Target URI</b> table attribute you want to delete, then select <b>Delete Table Attribtute</b> from the Tables menu.</li> <li>Click <b>OK</b>.</li> </ol> <p>End of procedure.</p>           |

| If you want to ...                 | then ...   |
|------------------------------------|--|
| Delete a P-NAPTR Target URI table, | <p>Note: Before you <i>delete</i> a P-NAPTR Target URI profile table, you must make sure that all related records have been deleted from the P-NAPTR Region.</p> <ol style="list-style-type: none"><li>1. Select the <b>P-NAPTR Target URI</b> table you want to delete, then select <b>Delete Table</b> from the Tables menu. The following message is displayed:<br/>Please delete all the records of this table prior to delete</li><li>2. Click <b>OK</b>.</li></ol> <p><i>End of procedure.</i></p> |

Note: Whenever a P-NAPTR Target URI is entered, the input will be translated into lowercase characters.

4 Define the **P-NAPTR Target URI Id**.

5 For more information on the parameter description, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# iAGCF provisioning

## Overview

### Purpose

This section provides the procedures that are used to provision the interface to the Integrated Access Gateway Control Function (iAGCF).

### Contents

|  |                       |
|--|-----------------------|
| <a href="#">Introduction to the base configuration</a> | <a href="#">4-261</a> |
|--|-----------------------|

# Introduction to the base configuration

## Introduction

The base configuration is the configuration phase where an LCP is configured to accommodate the nodes (also referred to as functions) in the IP Multimedia Service (IMS) architecture.

The base configuration is carried out by running the base configuration tool, which is a script that configures the IMS nodes and their required data tables without the use of the Graphical User Interface of the Feature server (FS GUI). This tool provides base configuration to a point where the Operation and Maintenance Center (OMC-P) can take over; when the tool has been run, communication is established and the OMC-P can be used to complete the setup, which includes digit analysis tables, routing tables, and Customer Premises Equipment (CPE) profile tables.

**Note:** The base configuration tool is only available for Alcatel-Lucent personnel.

## Using the FS GUI

Accessing the data tables using the Graphical User Interface of the Feature Server GUI (FS GUI) provides the ability to verify the data during troubleshooting. Important! Note that the FS GUI should only be used as read-only, changes have to be made using the OMC-P.

## iAGCF Profile

The iAGCF Profile contains parameter values that are applied to the iAGCF SIPia ports that are assigned to the particular profile record. Records will be sent to all IMS services. Emergency Services will always be supported by the iAGCF. At least one entry must exist in the Emergency Identifiers List in order to create an iAGCF profile.

## iAGCF Digit Map

The iAGCF Digit Map contains the Digit Map Names that are defined on the actual gateway itself via any interface used on the actual gateway to define digit map names. The name defined in this table are used in the iAGCF Gateway table to indicate which Digit Map should be used for all subscribers on the gateway.

## iAGCF Gateway Variant

The iAGCF Gateway Variant table contains parameter values that are applied to iAGCF Gateways. For reconfigurations of an IMS service and on manual updates to this table, the data is sent to the IMS service(s) associated with the iAGCF gateway(s) that are using the variant records. If the variant record is not used, no data is sent to any IMS services.

## iAGCF Gateway

The iAGCF Gateway table contains data specific to an iAGCF Gateway. Each iAGCF Gateway record is assigned to an iAGCF SIPia component. An iAGCF Gateway can only be assigned to one iAGCF SIPia component. iAGCF Gateway IDs are in the range of 2048 – 502047.

# SIP permanent linksets provisioning

## Overview

### Purpose

SIP Permanent Linksets are SIP signaling links between two SIP nodes that are permanently setup by provisioning.

The benefit of setting up SIP Permanent Linksets are as follows:

- The connectivity or transport state between the SIP servers is continuously monitored even when there is no call processing traffic. The status of the connection is graphically reported on the MI-Agent and when a failure is detected, an alarm is generated.
- In a connection oriented transport (TCP or SCTP), when the system starts, a connection is established for each link provisioned in the Linkset. This connection will be used and shared by all SIP transactions between the two connected nodes.

**Note:** In some cases, each node can establish its own *single* connection toward its peer, so there can actually be two connections.

### Contents

|   |       |
|---|-------|
| <a href="#">To provision an SIP Linkset</a>                 | 4-264 |
| <a href="#">To provision an SIP Permanent Linkset Group</a> | 4-269 |

# To provision an SIP Linkset

## Purpose

This procedure is used to provision an SIP Linkset.

## Steps to provision an SIP Linkset table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → SIP Tables** and expand the **SIPLinkset** folder.
- .....
- 2 In the left pane, expand the **SIPLinkset** folder to display the tables. If the folder is empty, add a **SIPLinkset** table.

| 3 | If you want to...                        | Then...  |
|---|--|--|
|   | add an SIP Linkset table,                | <ol style="list-style-type: none"> <li>1. Right-click <b>SIP Linkset</b> and select <b>Add Table</b>.</li> <li>2. Provide a <b>Table Number</b> and a <b>Table Name</b> in the <b>Add SIP Linkset table</b>.</li> <li>3. Click <b>OK</b>.</li> <li>4. Proceed to <a href="#">Step 4</a>.</li> </ol>        |
|   | modify (or rename) an SIP Linkset table, | <ol style="list-style-type: none"> <li>1. Select the table you want to modify.</li> <li>2. Right-click and select <b>Rename Table</b>.</li> <li>3. Modify the name and click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p>   |
|   | delete an SIP Linkset table,             | <ol style="list-style-type: none"> <li>1. Select the table you want to delete.</li> <li>2. Right-click and select <b>Delete Table</b>.</li> <li>3. Click <b>OK</b> to confirm deletion.</li> </ol> <p><b>Note:</b> An SIP Linkset must be locked before it can be deleted.</p> <p><i>End of steps.</i></p> |

- 4 Double-click the SIP Linkset table.

**Result:** The SIP Linkset table attributes window is displayed on the right-pane .

| 5 | If you want to ...                        | Then ...   |
|---|---|--|
|   | add attributes to an SIP Linkset table    | <ol style="list-style-type: none"> <li>Right-click on the SIP Linkset table attributes window and select <b>Add Table Attribute</b>.<br/><b>Result:</b> The <b>SIP Linkset</b> window is displayed.</li> <li>Proceed with <a href="#">Step 6</a>.</li> </ol>   |
|   | modify attributes of an SIP Linkset table | <ol style="list-style-type: none"> <li>Right-click the desired SIP Linkset and click <b>Modify Table Attribute</b>.<br/><b>Result:</b> The <b>SIP Linkset</b> window is displayed.</li> <li>Proceed with <a href="#">Step 6</a>.</li> </ol> <p><b>Note:</b> The SIP Linkset must be locked before it can be modified.</p>                                      |
|   | delete attributes of an SIP Linkset table | <ol style="list-style-type: none"> <li>Right-click the desired SIP Linkset and click <b>Delete Table Attribute</b>.</li> <li>Click <b>Ok</b> to confirm deletion.<br/><b>Note:</b> The SIP Linkset must be locked before it can be deleted and must not be in use by a Permanent Linkset Group when it is being deleted.</li> </ol> <p><i>End of steps</i></p> |

6 Provision the following parameters:

| Parameter         | Description   |
|-------------------|---|
| <b>Linkset ID</b> | By default, the smallest available integer number is provided by the system as <b>Linkset ID</b> for the SIP Linkset Profile.<br><b>Note:</b> If required this number can be changed to a higher value.   |
| <b>DNS</b>        | Check or clear the <b>DNS</b> check box. <ul style="list-style-type: none"> <li>If you want to use DNS to resolve the Destination FQDN, then select the <b>DNS</b> check box.</li> <li>If you want to configure IP(s) directly, then clear the <b>DNS</b> check box.</li> </ul> |

| Parameter  | Description   |
|--|---|
| <b>Transport</b>                                   | <p>Select the transport protocol type in the <b>Transport</b> field.</p> <p>The following are the three types of transport protocol:</p> <ul style="list-style-type: none"> <li>• <b>TCP</b></li> <li>• <b>UDP</b></li> <li>• <b>SCTP</b></li> </ul>  |
| <b>TLS</b>   | <p>Enable the <b>TLS</b> check box.</p> <p><b>Note:</b> The <b>TLS</b> check box can only be checked when "transport" is set to TCP while for UDP and SCTP, this TLS field is unavailable.</p> <p><b>Note:</b> TLS can only be enabled when NI 1 type is Default.</p>   |
| <b>User part of R-URI and TO header in OPTIONS</b> | <p>Enter the appropriate value in the <b>User part of R-URI and TO header in OPTIONS</b> field.</p>   |
| <b>User part of FROM header in OPTIONS</b>         | <p>Enter the appropriate value in the <b>User part of FROM header in OPTIONS</b> field.</p> <p><b>Note:</b> When any one or both of the fields <b>User part of R-URI and TO header in OPTIONS</b> and <b>User part of FROM header in OPTIONS</b> are provisioned, the user part of the associated headers in the heart beat OPTIONS message is added by the string configured in the associated fields.</p> |
| <b>Enable Symmetric Connection</b>                 | <p>Check <b>Enable Symmetric Connection</b> to enable symmetric connection to the given Linkset.</p> <p><b>Note:</b> The default value is cleared and can be changed only when the <b>Transport</b> protocol is set to <b>SCTP</b>.</p>   |
| <b>Load Sharing</b>                                | <p>Check the <b>Load Sharing</b> check box if load sharing is supported.</p> <p><b>Note:</b> Enabling load sharing for UDP and TCP will distribute SIP messages in a round-robin fashion to each of the provisioned Destination IP Addresses. <b>Load Sharing</b> does not apply to SCTP Linksets.</p>  |

| Parameter                       | Description  |
|---------------------------------|--|
| <b>SIP Heart Beat</b>           | <p>Check <b>SIP Heart Beat</b>, if the link status needs to be checked via SIP heartbeat messages.</p> <p><b>Note:</b> When the transport type is <b>SCTP</b>, the default value is <i>unchecked</i> and can be changed. When the transport type is <b>TCP</b> or <b>UDP</b>, the default value is <i>checked</i> and cannot be changed.</p> |
| <b>SCTP Profile</b>             | <p>If <b>SCTP</b> is selected as the <b>Transport</b> type, <b>SCTP Profile</b> field can be used to associate the SIP Linkset with an SCTP profile.</p> <p><b>Note:</b> SCTP Parameter Profile must have already been provisioned. For more information refer to “<a href="#">To provision an SCTP Profile</a>” (p. 10-37).</p>             |
| <b>Admin State</b>              | <p><b>Admin State</b> field is used to lock or unlock a linkset.</p>   |
| <b>NI 1 and NI 2</b>            | <p>Select <b>NI 1</b> and <b>NI 2</b> values.</p> <p><b>Note:</b> The allowed values for <b>NI 1</b> are <i>Default</i> and <i>Publish</i>. For <b>NI 2</b>, the value is <i>None</i>.</p> <p><i>Publish</i> is only applicable for P-CSCF and IBCF.</p>   |
| <b>Destination FQDN</b>         | <p>If necessary, enter a <b>Destination FQDN</b> (for example: icsf-stdn.dv312.lab.com).</p> <p><b>Note:</b> This field is mandatory when <b>DNS</b> is checked and optional when <b>DNS</b> is cleared.</p>   |
| <b>Destination IP Addresses</b> | <p>If DNS is not used, assign at least one IP address in <b>Destination IP Addresses</b> to define the destination.</p> <p>Select either <b>IPv4</b> or <b>IPv6</b> in the <b>IP Type</b> field to specify the type of destination IP address.</p>   |
| <b>Port</b>                     | <p>If DNS is not used, enter the number of the IP port used to communicate with the far-end SIP destination in the <b>Port</b> field.</p>  |

| Parameter  | Description  |
|------------|--|
| IP Address | <p>Enter the destination IPv4 or IPv6 address (as selected in the <b>IP Type</b> field) in the <b>IP Address</b> field.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• The destination IP address must be <i>unique</i>.</li> <li>• When both Destination FQDN and Destination IP Address(es) are provisioned, the FQDN is matched with the SIP Request-URI. If a match is found, the Destination IP Address(es) are used instead of performing a real DNS lookup.</li> <li>• If the <b>Transport</b> type is <i>SCTP</i>, then the Destination IP Address(es) must be the IP address(es) of the remote host to which an SCTP association will be formed. If more than one IP address is used, then the remote is considered multi-homed.</li> </ul> |

- 7 Click **Add** to add the IP address to the Destination IP Addresses list.

**Note:**

- To add another IP address to the list, see the parameter description for **Destination IP Addresses** in the table above.
- To remove an IP address from the list, select the IP address and click **Remove**.
- **Add** and **Remove** functionality are applicable only during the initial configuration. IP addresses cannot be changed after the SIP Linkset is added.

- 8 Click **OK**.

**Result:** The SIP Linkset is added or modified.

For further information on the parameters, refer the topic “SIP LinkSet Profiles” in the *Alcatel-Lucent Control Platform 1800/1000/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision an SIP Permanent Linkset Group

## Purpose

This procedure is used to provision an SIP Permanent Linkset Group.

The purpose of creating an SIP Permanent Linkset Group (PLG) is to group linksets or destinations with similar characteristics and to monitor the linksets or destinations.

For example, the S-CSCF connects to an Application Server, therefore, a PLG containing linksets that represent the application server can be created and assigned to the S-CSCF . Similarly, other application functions like I-CSCF, BGCF, IBCF, and so on connecting to different application servers can be grouped into different PLGs.

## Before you begin

Points to remember:

- A *maximum* of sixteen tables are allowed under the SIP Permanent Linkset Group.
- A *maximum* of 512 Linkset Ids are allowed per given SIP Permanent Linkset Group entry.

## Steps to provision an SIP Permanent Linkset Group

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → SIP Tables** .

**Result:** The **SIP Tables** window is displayed.

- 2 In the left pane, expand the **SIP Permanent Linkset Group** folder to display the tables. If the folder is empty, add an SIP Permanent Linkset Group table.

| 3 | If you want to... | then...   |
|---|-------------------|---|
|   | add a table,      | <ol style="list-style-type: none"><li>1. Right-click on <b>SIP Permanent Linkset Group</b> and select <b>Add Table</b>.</li><li>2. Enter a <b>Table Number</b> and a <b>Table Name</b>.</li><li>3. Click <b>OK</b>.</li><li>4. Proceed with <a href="#">Step 4</a>.</li></ol> |

| If you want to...          | then...  |
|----------------------------|--|
| modify (= rename) a table, | <ol style="list-style-type: none"> <li>Select the table you want to modify.</li> <li>Right-click and select <b>Rename Table</b></li> <li>Modify the name and click <b>OK</b>.</li> </ol> <p><i>End of procedure.</i></p> |
| delete a table,            | <ol style="list-style-type: none"> <li>Select the table you want to delete.</li> <li>Right-click and select <b>Delete Table</b></li> <li>Click <b>OK</b> to confirm deletion.</li> </ol> <p><i>End of procedure.</i></p> |

- 
- 4 Double-click on the table to provision, or right-click and select **Open**.

**Result:** The **SIP Permanent Linkset Group** populates in the right pane.

---

| 5 If you want to ...                                      | then ...  |
|---|---|
| add attributes to SIP Permanent Linkset Group table       | <ol style="list-style-type: none"> <li>Right-click on the desired SIP Permanent Linkset Group table and select <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Permanent Linkset Group</b> window is displayed.</li> <li>Proceed with <a href="#">Step 6</a>.</li> </ol>   |
| modify attributes of an SIP Permanent Linkset Group table | <ol style="list-style-type: none"> <li>Right-click on the desired SIP Permanent Linkset Group table and select <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Permanent Linkset Group</b> window is displayed.</li> <li>Proceed with <a href="#">Step 6</a></li> </ol> |

- 
- 6 Select the **Linkset Id** for the **SIP Permanent Linkset Group**.

**Note:** The **Linkset ID** field provides a drop-down list of available Linkset Ids.

- 
- 7 Click **OK**.

---

For more information on the parameter description, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

E N D   O F   S T E P S

---

# Provisioning diameter multiple destination FQDNs

## Overview

### Purpose

This section provides the procedures that are used to provision the Diameter Multiple Destination FQDNs, and the conversion procedure from Diameter Geographic Redundancy and vice versa.

### Contents

|  |       |
|--|-------|
| Conversion from Diameter Geo-redundancy to support Multiple destinations | 4-273 |
| Conversion from Multiple destination to support Diameter Geo-redundancy  | 4-276 |
| To provision a Diameter Multiple Destination Profile                     | 4-278 |

# Conversion from Diameter Geo-redundancy to support Multiple destinations

## Purpose

This procedure is used to convert the configuration from diameter geo-redundancy to support multiple destinations.

**Note:** This conversion procedure can be executed only when geographic redundancy is already in use and the subscriber data or user profiles are distributed over multiple HSSs.

## Before you begin

Observe the following:

- The SLFs have to be provisioned prior to doing the conversion from geo-redundancy to the Multiple destinations configuration.
- The conversion procedures should only be executed when the Software Upgrade is done and Diameter geo-redundancy configuration are working.
- Diameter Cx /Sh messages can be evenly distributed to HSSs based on the per call basis.
- To ensure a safe conversion to multiple destinations, the following provisioning sequences are recommended to be followed and the cautions observed.



### NOTICE

#### Service-disruption hazard

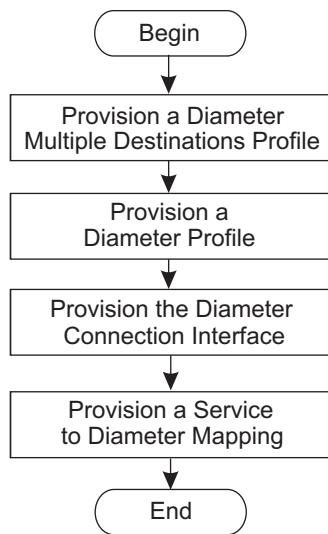
*This procedure can be service affecting. During the conversion, all the Diameter connections will be torn down and the new connections will be re-established after the service to Diameter mapping is provisioned.*

*To minimize the service impact, the user should observe the following:*

- *The conversion from geo-redundancy to multiple destinations for IMS service should be done one by one.*
- *After provisioning the service to Diameter mapping for Multiple destinations, make sure that the Diameter connections work well. Only then provision the next IMS service to Diameter Mapping for multiple destinations.*
- *Do not delete any existing Diameter profiles. Only add new Diameter profiles. This enables you to switch back to geo-redundancy configuration, if the conversion fails.*
- *During this conversion process, no other FSGUI provisioning is allowed.*

## Conversion task flow diagram

The following diagram describes the provisioning sequence for conversion to support multiple destinations:



## Conversion from Diameter Geo-redundancy to support Multiple destinations

Perform the following steps:

- 1 Provision a Diameter Multiple Destinations Profile.

Refer to “[To provision a Diameter Multiple Destination Profile](#)” (p. 4-278).

- 2 Provision a Diameter Profile.

Refer to “[To provision a Diameter profile](#)” (p. 10-23).

- 3 Provision the Diameter Connection Interface.

Provision the Application Type “Cx” or “Sh” and select the Diameter Multiple Destinations Profile ID. Refer to “[To provision a Diameter profile](#)” (p. 10-23).

- 4 Provision Service to Diameter Mapping.

Provision the IMS service to the Diameter Profile. Refer to “[To provision a Service to Diameter mapping](#)” (p. 10-32).

**Note:** After provisioning the service to Diameter mapping for Multiple destinations, make sure that the Diameter connections are working. For example, the user can do some registrations or calls to make sure that the Diameter connections are working, and the registrations or calls can be distributed to the remote SLF/HSS servers correctly.

| If...  | Then...  |
|--|--|
| the Diameter Connection for Multiple Destinations works on this IMS service,         | map the next IMS service to this profile.  |
| the Diameter Connection for Multiple Destinations does not work on this IMS service, | switch back to the geo-redundancy configuration (that is, map the service back to the old profile) and fix the issues, then repeat this procedure. |

# Conversion from Multiple destination to support Diameter Geo-redundancy

## Purpose

This procedure is used to convert the configuration from diameter multiple destinations to diameter geo-redundancy.

**Note:** This conversion procedure can be executed only when Diameter multiple destinations configuration is already in use.

## Before you begin

Observe the following:

- The conversion procedures should only be executed when the Software Upgrade is done and Diameter multiple destinations configuration is working.
- Diameter Cx /Sh messages can be evenly distributed to SLF/HSSs based on the per call basis.
- To ensure a safe conversion to geo-redundancy, the following provisioning sequences are recommended to be followed and the cautions observed.



### NOTICE

#### Service-disruption hazard

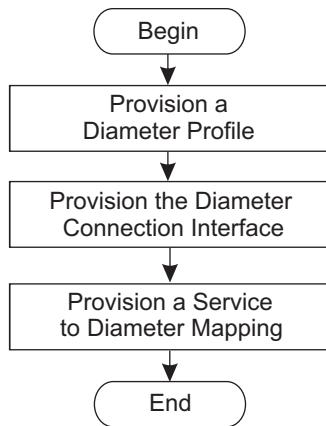
*This procedure can be service affecting. During the conversion all the Diameter connections will be torn down and the new connections will be re-established after the service to Diameter mapping is provisioned.*

*To minimize the service impact, the user should observe the following:*

- *The conversion from Diameter multiple destinations to geo-redundancy for IMS service should be done one by one.*
- *After provisioning the service to Diameter mapping for geo-redundancy, make sure that the Diameter connections are working. Only then provision the next IMS service to Diameter Mapping for geo-redundancy.*
- *Do not delete any existing Diameter profiles. Only add new Diameter profiles. This enables you to switch back to multiple destinations configuration, if the conversion fails.*
- *During this conversion process, no other FSGUI provisioning is allowed.*

## Conversion task flow diagram

The following diagram describes the provisioning sequence for conversion to support geographic redundancy:



### Conversion from Multiple destination to support Diameter Geo-redundancy

Perform the following steps:

**1** Provision a Diameter Profile.

Refer to “[To provision a Diameter profile](#)” (p. 10-23).

**2** Provision the Diameter Connection Interface.

Provision the Cx/Sh Diameter Connection Interface with Geographic Redundancy configuration. Refer to “[To provision a Diameter profile](#)” (p. 10-23).

**3** Provision Service to Diameter Mapping.

Provision the IMS service to the Diameter Profile. Refer to “[To provision a Service to Diameter mapping](#)” (p. 10-32).

**Note:** After provisioning the service to Diameter mapping for Geographic Redundancy, make sure that the Diameter connections work well.

| If...  | Then...   |
|--|---|
| the Diameter Connection for Geographic Redundancy works on this IMS service,         | map the next IMS service to this profile.   |
| the Diameter Connection for Geographic Redundancy does not work on this IMS service, | switch back to the Multiple destinations configuration (that is, map the service back to the old profile) and fix the issues, then repeat this procedure. |

# To provision a Diameter Multiple Destination Profile

## Purpose

This procedure is used to add, modify, or delete a Diameter Multiple Destination Profile.

The purpose of creating a Diameter Multiple Destination Profile is to define the FQDN list. The Destination FQDN can be provisioned either as an Agent (a default CCF), a backup server or the final server.

## Before you begin

Each Diameter Multiple Destination Profile can contain up to 16 FQDN List (tables).

## Steps to provision a Diameter Multiple Destination Profile table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS** → **IMS Tables** → **IMS** → **General** and expand the **Diameter Multiple Destination Profile** folder.

**Note:** If no Diameter Multiple Destination Profile table is provisioned then you need to add a new table.

- 
- 2 Perform the following steps to add, rename, or delete a Diameter Multiple Destination Profile :

| If you want to...   | Then...  |
|---|--|
| add a Diameter Multiple Destination Profile table,                | <ol style="list-style-type: none"> <li>1. Right click on <b>Diameter Multiple Destination Profile</b> and select <b>Add Table</b>.</li> <li>2. Provide a <b>Table Number</b> and a <b>Table Name</b> in the <b>Add Diameter Multiple Destination Profile</b> table.</li> <li>3. Click <b>OK</b>.</li> <li>4. Proceed to <a href="#">Step 3</a>.</li> </ol> |
| modify (or rename) a Diameter Multiple Destination Profile table, | <ol style="list-style-type: none"> <li>1. Select the table you want to modify.</li> <li>2. Right-click and select <b>Rename Table</b></li> <li>3. Modify the name and click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p>  |

| If you want to...                                     | Then...  |
|---|--|
| delete a Diameter Multiple Destination Profile table, | <ol style="list-style-type: none"> <li>1. Select the table you want to delete.</li> <li>2. Right-click and select <b>Delete Table</b>.</li> <li>3. Click <b>OK</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

**3** Double-click the Diameter Multiple Destination Profile table.

**Result:** The Diameter Multiple Destination Profile table attributes are displayed in the right-pane.

| 4 | If you want to ...  | Then ...   |
|---|---|--|
|   | add attributes to a Diameter Multiple Destination Profile table,    | <ol style="list-style-type: none"> <li>1. Right-click in the Diameter Multiple Destination Profile table attributes screen and select <b>Add Table Attribute</b>.<br/><b>Result:</b> The <b>Diameter Multiple Destination Profile</b> screen is displayed.</li> <li>2. Proceed with <a href="#">Step 5</a>.</li> </ol> |
|   | modify attributes of a Diameter Multiple Destination Profile table, | <ol style="list-style-type: none"> <li>1. Right-click the desired Diameter Multiple Destination Profile and click <b>Modify Table Attribute</b>.<br/><b>Result:</b> The <b>Diameter Multiple Destination Profile</b> screen is displayed.</li> <li>2. Proceed with <a href="#">Step 5</a>.</li> </ol>                  |
|   | delete attributes of a Diameter Multiple Destination Profile table, | <ol style="list-style-type: none"> <li>1. Right-click the desired Diameter Multiple Destination Profile and click <b>Delete Table Attribute</b>.</li> <li>2. Click <b>Ok</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p>  |

**5** Provision the following parameters:

| Parameter               | Description  |
|-------------------------|--|
| <b>FQDN Index</b>       | <b>FQDN Index</b> field by default displays the least unique number available.<br><b>Note:</b> This field is disabled and cannot be modified.  |
| <b>Destination FQDN</b> | Enter the destination FQDN in the <b>Destination FQDN</b> field.<br><b>Note:</b> The destination FQDN can be an explicit IP address or a fully qualified domain name.  |
| <b>Agent</b>            | Enable the <b>Agent</b> check box, if the destination FQDN is an agent, that is standalone SLF.<br><b>Note:</b> <ol style="list-style-type: none"> <li>If the destination FQDN is HSS, then clear the <b>Agent</b> field.</li> <li>If the <b>Agent</b> field is checked for a provisioned FQDN, then the selected FQDN is used to send an ACR message when there is no CCF address passed from an application such as CTS in the ACR message.</li> </ol>   |
| <b>Destination Port</b> | Enter the destination port number in the <b>Destination Port</b> field.  |
| <b>Backup FQDN</b>      | Select the <b>Backup FQDN</b> check box for an FQDN, if required.<br><b>Note:</b> <ol style="list-style-type: none"> <li>The FQDN with the <b>Backup FQDN</b> field checked is used to send ACR, if the CCF address provided by HSS does not match with the provisioned FQDN.</li> <li>Ensure that the <b>Backup FQDN</b> is selected for at least one of the FQDNs. If no Backup FQDN is selected for any of the FQDNs, the ACR is buffered until it is sent to the ABF and the temporary buffer is at least 90% full.</li> </ol> |

| Parameter                  | Description   |
|----------------------------|---|
| <b>Geo-Redundancy Type</b> | This field is used to support Primary and Alternate SLF destinations with geo-redundancy capability. One or more Primary FQDNs, and one or more Alternate FQDNs are allowed to be selected as SLF destinations in a diameter profile for Dx/Dh/Sh interface within the provisioned MDL. Dx/Dh/Sh messages are first routed to Primary SLF destinations by means of round robin. When all the provisioned primary SLF destinations are not available (100 per cent) in the MDL, the Diameter Dx/Dh/Sh messages are routed to the Alternate SLF destinations by means of round robin. |

**6** Click **OK**.

**Result:** The Diameter Multiple Destination Profile attribute is added or modified.

For more information about the parameters, refer to the topic “Diameter Multiple Destinations Profile Table” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# Border gateway provisioning

## Overview

### Purpose

This section provides the procedures that are used to provision the Border Gateway.

### Contents

|   |       |
|---|-------|
| To provision a Core Bearer Realm                | 4-283 |
| To provision a Published Realm                  | 4-286 |
| To assign a Published Realm to a Border Gateway | 4-290 |

# To provision a Core Bearer Realm

## Purpose

This procedure is used to provision a Core Bearer Realm.

## Before you begin

A record in the Core Bearer Realm table cannot be modified or deleted if it is being used as a Core Primary Bearer Realm or Core Alternate Bearer Realm in the Published Realm table.

## Steps to provision a Core Bearer Realm

Perform the following steps at the Provisioning GUI.

- 1 Select IMS → Global Tables.

**Result:** The Global Tables window is displayed.

- 2 In the left pane, expand the **Core Bearer Realm** folder to display the tables. If the folder is empty, add a Core Bearer Realm table.

- 3 Perform the following steps in the **Global Tables** window to add, rename, or delete a **Core Bearer Realm**:

| If you want to...                                       | then...  |
|---|--|
| add a table in the <b>Core Bearer Realm</b> folder      | <ol style="list-style-type: none"><li>1. Right-click <b>Core Bearer Realm</b> and select <b>Add Table</b>.</li><li>2. Select a unique number from the <b>Table Number</b> drop-down list.</li><li>3. Enter a unique name in the <b>Table Name</b> field.</li><li>4. Click <b>OK</b>.<br/><i>End of procedure</i></li></ol> |
| rename the table in the <b>Core Bearer Realm</b> folder | <ol style="list-style-type: none"><li>1. Right-click on the desired table and select <b>Rename Table</b>.</li><li>2. Enter the required table name and click <b>OK</b>.<br/><i>End of procedure</i></li></ol>  |

| If you want to...                                       | then...   |
|---|---|
| delete the table in the <b>Core Bearer Realm</b> folder | <ol style="list-style-type: none"> <li>Right-click on the desired table and select <b>Delete Table</b>.</li> <li>Click <b>Yes</b> to confirm the deletion.<br/><i>End of procedure</i></li> </ol> |

- 4 Double-click the desired Core Bearer Realm table. The Core Bearer Realm table opens in the right pane. Perform the following steps to add, modify, or delete the Core Bearer Realm table attributes:

| If you want to...                                | then...   |
|--|---|
| add <b>Core Bearer Realm</b> table attributes    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol>  |
| modify <b>Core Bearer Realm</b> table attributes | <p>Perform the following steps.</p> <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.</li> <li>Enter a name in the <b>Core Bearer Realm Name</b> field.<br/><b>Note:</b> The Core Bearer Realm name should be unique across all records.<br/><i>End of procedure</i></li> </ol> |
| delete <b>Core Bearer Realm</b> table attributes | <p>Perform the following steps.</p> <ol style="list-style-type: none"> <li>Right-click the desired profile and select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm.<br/><i>End of procedure</i></li> </ol>  |

- 5 Provision the following parameters:

| Parameter                   | Description   |
|-----------------------------|---|
| <b>Core Bearer Realm ID</b> | Select a unique number in the <b>Core Bearer Realm ID</b> drop-down list. |

| Parameter                     | Description  |
|-------------------------------|--|
| <b>Core Bearer Realm Name</b> | Enter a name in the <b>Core Bearer Realm Name</b> field.<br><b>Note:</b> The Core Bearer Realm name should be unique across all records. |

- 6 Click **OK**.

**Result:** A new Core Bearer Realm is added.

For more information on the parameter description, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision a Published Realm

## Purpose

This procedure is used to provision a Published Realm.

## Before you begin

A record in the Published Realm table cannot be modified or deleted if it is being used or assigned to P-CSCF or iAGCF Profile.

A record in the Published Realm table cannot be modified or deleted if it is being used in the Border Gateway Published Realm Assignment table.

## Steps to provision a Published Realm

Perform the following steps at the Provisioning GUI.

- 1 Select **IMS → Global Tables**.

**Result:** The **Global Tables** window is displayed.

- 2 In the left pane, expand the **Published Realm** folder to display the tables. If the folder is empty, add a Published Realm table.
- 3 Perform the following steps in the **Global Tables** window to add, rename, or delete a **Published Realm**:

| If you want to...                                     | then...   |
|---|---|
| add a table in the <b>Published Realm</b> folder      | <ol style="list-style-type: none"> <li>1. Right-click <b>Published Realm</b> and select <b>Add Table</b>.</li> <li>2. Select a unique number from the <b>Table Number</b> drop-down list.</li> <li>3. Enter a unique name in the <b>Table Name</b> field.</li> <li>4. Click <b>OK</b>.<br/><i>End of procedure</i></li> </ol> |
| rename the table in the <b>Published Realm</b> folder | <ol style="list-style-type: none"> <li>1. Right-click on the desired table and select <b>Rename Table</b>.</li> <li>2. Enter the required table name and click <b>OK</b>.<br/><i>End of procedure</i></li> </ol>  |

| If you want to...                                     | then...   |
|---|---|
| delete the table in the <b>Published Realm</b> folder | <ol style="list-style-type: none"> <li>Right-click on the desired table and select <b>Delete Table</b>.</li> <li>Click <b>Yes</b> to confirm the deletion.<br/><i>End of procedure</i></li> </ol> |

- 4 Double-click the desired Published Realm table. The Published Realm table opens in the right pane. Perform the following steps to add, modify, or delete the Published Realm table attributes:

| If you want to...                              | then...   |
|--|---|
| add <b>Published Realm</b> table attributes    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol>  |
| modify <b>Published Realm</b> table attributes | <p>Perform the following steps.</p> <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of procedure</i></li> </ol> |
| delete <b>Published Realm</b> table attributes | <p>Perform the following steps.</p> <ol style="list-style-type: none"> <li>Right-click the desired profile and select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm.<br/><i>End of procedure</i></li> </ol>  |

- 5 Provision the following parameters:

| Parameter                   | Description  |
|-----------------------------|--|
| <b>Published Realm ID</b>   | Select a unique number in the <b>Published Realm ID</b> drop-down list.  |
| <b>Published Realm Name</b> | Enter a name in the <b>Published Realm Name</b> field.<br><b>Note:</b> The Published realm name should be unique across all records. |
| <b>IP Version</b>           | Select the IP version from the <b>IP Version</b> drop-down list.   |

| Parameter                          | Description   |
|------------------------------------|---|
| <b>Signaling v4 VLAN</b>           | <p><b>Note:</b> Before provisioning the P-CSCFs to use the IP v4 VLAN IDs, the signaling network must already be setup with the VLANs.</p> <p>Select the Signaling v4 VLAN from the <b>Signaling v4 VLAN</b> drop-down list.</p> <p>A change can be made to the following if all the PCSCFs using the published realm are locked (or the services associated with the PCSCFs are locked). This allows a change to the Signaling v4 VLAN value without having to delete all the PCSCF SIPia ports. The FEPH in the architecture, is also involved in this functionality.</p> <ul style="list-style-type: none"> <li>• change to the actual Signaling v4 VLAN value in the Published Realm table</li> <li>• change to the PCSCF profile's Published Realm ID assignment</li> <li>• change to the SIPia's Port Profile assignment</li> </ul> <p>To assign the Published Realm ID to a PCSCF Profile, see “<a href="#">To provision PCSCF profile</a>” (p. 4-77)</p> <p>To assign the PCSCF Profile to a PCSCF SIPia port, see “<a href="#">To provision a SIPia port</a>” (p. 10-40)</p> |
| <b>Core Primary Bearer Realm</b>   | <p>Select the primary bearer realm from the <b>Core Primary Bearer Realm</b> drop-down list.</p> <p>To provision a core bearer realm, see “<a href="#">To provision a Core Bearer Realm</a>” (p. 4-283).</p>  |
| <b>Core Alternate Bearer Realm</b> | <p>Select the alternate bearer realm from the <b>Core Alternate Bearer Realm</b> drop-down list.</p>  |
| <b>Bypass IPv4 Domain Suffix</b>   | <p>Enter the necessary data in the <b>Bypass IPv4 Domain Suffix</b> field.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• This field is disabled if <b>v6</b> is selected in the <b>IP Version</b> drop-down list.</li> <li>• If <b>v4/v6</b> is selected in the <b>IP Version</b> drop-down list and <b>Border Gateway Bypass</b> is enabled in the SBLP profile, then both <b>Bypass IPv4 Domain Suffix</b> and <b>Bypass Ipv6 Domain Suffix</b> fields cannot be left blank at the same time.</li> </ul>   |

| Parameter                 | Description   |
|---------------------------|---|
| Bypass IPv6 Domain Suffix | <p>Enter the necessary data in the <b>Bypass IPv6 Domain Suffix</b> field.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"><li>• This field is disabled if <b>v4</b> is selected in the <b>IP Version</b> drop-down list</li><li>• If <b>v4/v6</b> is selected in the <b>IP Version</b> drop-down list and <b>Border Gateway Bypass</b> is enabled in the SBLP profile, then both <b>Bypass IPv4 Domain Suffix</b> and <b>Bypass Ipv6 Domain Suffix</b> fields cannot be left blank at the same time.</li></ul> |

6 Click OK.

**Result:** A new Published realm is added.

For more information on the parameter description, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To assign a Published Realm to a Border Gateway

## Purpose

This procedure provides the steps to assign a Published realm to a Border Gateway (BGW).

## Steps to assign a Published realm to a Border Gateway (BGW)

Perform the following steps at the Provisioning GUI.

- 1 Select **IMS → Global Tables**.

**Result:** The **Global Tables** window is displayed.

- 2 In the left pane, expand the **Border Gateway Published Realm Assignment** folder to display the tables. If the folder is empty, add a **Border Gateway Published Realm Assignment** table.
- 3 Perform the following steps in the **Global Tables** window to add, rename, or delete a **Border Gateway Published Realm Assignment**:

| If you want to...   | then...   |
|---|---|
| add a table in the <b>Border Gateway Published Realm Assignment</b> folder      | <ol style="list-style-type: none"> <li>1. Right-click <b>Border Gateway Published Realm Assignment</b> and select <b>Add Table</b>.</li> <li>2. Select a unique number from the <b>Table Number</b> drop-down list.</li> <li>3. Enter a unique name in the <b>Table Name</b> field.</li> <li>4. Click <b>OK</b>.<br/><i>End of procedure</i></li> </ol> |
| rename the table in the <b>Border Gateway Published Realm Assignment</b> folder | <ol style="list-style-type: none"> <li>1. Right-click on the desired table and select <b>Rename Table</b>.</li> <li>2. Enter the required table name and click <b>OK</b>.<br/><i>End of procedure</i></li> </ol>  |
| delete the table in the <b>Border Gateway Published Realm Assignment</b> folder | <ol style="list-style-type: none"> <li>1. Right-click on the desired table and select <b>Delete Table</b>.</li> <li>2. Click <b>Yes</b> to confirm the deletion.<br/><i>End of procedure</i></li> </ol>   |

- 4 Double-click the desired Border Gateway Published Realm Assignment table. The Border Gateway Published Realm Assignment table opens in the right pane. Perform the following steps to add, modify, or delete the Border Gateway Published Realm Assignment table attributes:

| If you want to...  | then...  |
|--|--|
| add <b>Border Gateway Published Realm Assignment</b> table attributes    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol>   |
| modify <b>Border Gateway Published Realm Assignment</b> table attributes | <p>Perform the following steps.</p> <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of procedure</i></p> |
| delete <b>Border Gateway Published Realm Assignment</b> table attributes | <p>Perform the following steps.</p> <ol style="list-style-type: none"> <li>Right-click the desired profile and select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm.</li> </ol> <p><i>End of procedure</i></p>  |

- 5 Provision the following parameters:

| Parameter                         | Description  |
|-----------------------------------|--|
| <b>Border Gateway</b>             | Select the Border Gateway from the <b>Border Gateway</b> drop-down list.   |
| <b>Available Published Realms</b> | Select the necessary realm from the <b>Available Published Realms</b> list and click <b>Add</b> .<br><br><b>Result:</b> The selected realm is moved to the <b>Selected Published Realms</b> list.                          |
| <b>Selected Published Realms</b>  | Repeat the previous step to add more realms to the <b>Selected Published Realms</b> list.<br><br><b>Note:</b> To remove a realm from the <b>Selected Published Realms</b> list, select the realm and click <b>Delete</b> . |

6 Click OK.

**Result:** A Published Realm is assigned to a Border Gateway .

For more information on the parameter description, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# Central Routing Function provisioning

## Overview

### Purpose

This section provides the task flow and the provisioning procedures for the Central Routing Function (CRF).

### Contents

|  |       |
|--|-------|
| CRF provisioning task flow                   | 4-294 |
| To provision a CRF Target table              | 4-297 |
| To provision a CRF Target List table         | 4-302 |
| To provision a CRF Treatment table           | 4-306 |
| To provision a CRF Digit Analysis Table      | 4-310 |
| To provision a CRF Trunk Group table         | 4-313 |
| To provision a CRF Route Plan table          | 4-316 |
| To provision a CRF Task Plan table           | 4-320 |
| To provision a CRF Route Priority List table | 4-324 |
| To provision a CRF Route Profile table       | 4-328 |

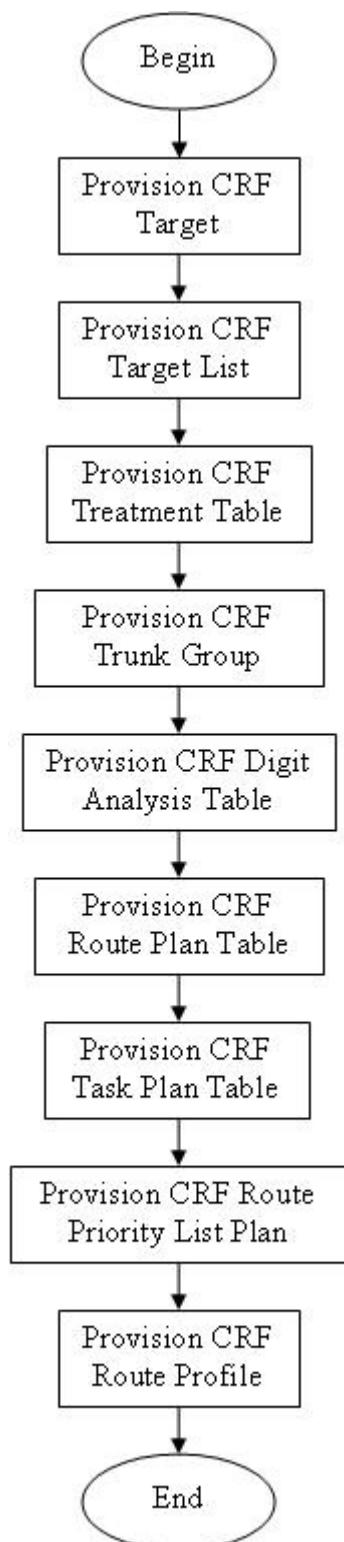
---

# CRF provisioning task flow

## Purpose

This topic provides the provisioning task flow that has to be followed to provision CRF Tables.

## Provisioning task flow diagram



## S-CSCF provisioning tasks

Perform the following steps to provision CRF Tables:

- 
- 1 Provision the CRF Target.

See “[To provision a CRF Target table](#)” (p. 4-297).

---

- 2 Provision the CRF Target List.

See “[To provision a CRF Target List table](#)” (p. 4-302).

---

- 3 Provision the CRF Treatment Table.

See “[To provision a CRF Treatment table](#)” (p. 4-306).

---

- 4 Provision the CRF Trunk Group Table.

See “[To provision a CRF Digit Analysis Table](#)” (p. 4-310).

---

- 5 Provision the CRF Digit Analysis Table.

See “[To provision a CRF Trunk Group table](#)” (p. 4-313).

---

- 6 Provision the CRF Route Plan Table.

See “[To provision a CRF Route Plan table](#)” (p. 4-316).

---

- 7 Provision the Task Plan Table.

See “[To provision a CRF Task Plan table](#)” (p. 4-320).

---

- 8 Provision the CRF Route Priority List Plan Table.

See “[To provision a CRF Route Priority List table](#)” (p. 4-324).

---

- 9 Provision the CRF Route Profile.

See “[To provision a CRF Route Profile table](#)” (p. 4-328).

# To provision a CRF Target table

## Purpose

This procedure is used to provision a CRF Target table.

## Steps to provision a CRF Target table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → CRF Tables**.

**Result:** The **CRF Tables** window is displayed.

- 2 In the left pane, expand the **CRF Target** folder.

**Result:** The CRF Target tables are listed under the folder in the left pane.

If the folder is empty, add a CRF Target table.

Perform the following steps in the **CRF Tables** window to add, rename, or delete a CRF Target table :

| If you want to ...         | then ...   |
|----------------------------|--|
| add a CRF Target table,    | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |
| rename a CRF Target table, | <ol style="list-style-type: none"><li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li><li>2. In the <b>Table Name</b> box, type a new table name.</li><li>3. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p>  |

| If you want to ...         | then ...  |
|----------------------------|---|
| delete a CRF Target table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a CRF Target table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the CRF Target table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **CRF Tables** window to add, modify, or delete the CRF Target table attributes:

| If you want to ...                    | then ...  |
|---------------------------------------|---|
| add the CRF Target table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a CRF Target table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                    | then ...  |
|---------------------------------------|---|
| delete a CRF Target table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter               | Description   |
|-------------------------|---|
| <b>Target ID</b>        | Select a unique ID for the CRF Target.<br>Range: 5001-7048<br>Default: Next available ID                          |
| <b>Description</b>      | Up to 32 characters   |
| <b>Address Type</b>     | IPv4/IPv6/Domain<br>Default: IPV4   |
| <b>Target Host Name</b> | IPv4 Address or IPv6 Address or Domain  |
| <b>Port</b>             | 0 - 65535<br>Default 5060   |
| <b>Admin State</b>      | Lock/Unlock<br>Default: Unlock<br><b>Note:</b> This field will be set to its default value and disabled in Rel26. |
| <b>Digit Table ID</b>   | IDs of IMS Digit Tables<br><b>Note:</b> This field will be set to its default value and disabled in Rel26.        |
| <b>Enable Heartbeat</b> | Yes/No<br>Default: No<br><b>Note:</b> This field will be set to its default value and disabled in Rel26.          |

| Parameter          | Description  |
|--------------------|--|
| <b>Audio</b>       | Yes/No<br>Default: No<br><b>Note:</b> This field will be set to its default value and disabled in Rel26. |
| <b>Video</b>       | Yes/No<br>Default: No<br><b>Note:</b> This field will be set to its default value and disabled in Rel26. |
| <b>Data</b>        | Yes/No<br>Default: No<br><b>Note:</b> This field will be set to its default value and disabled in Rel26. |
| <b>Application</b> | Yes/No<br>Default: No<br><b>Note:</b> This field will be set to its default value and disabled in Rel26. |
| <b>Message</b>     | Yes/No<br>Default: No<br><b>Note:</b> This field will be set to its default value and disabled in Rel26. |
| <b>Text</b>        | Yes/No<br>Default: No<br><b>Note:</b> This field will be set to its default value and disabled in Rel26. |
| <b>Control</b>     | Yes/No<br>Default: No<br><b>Note:</b> This field will be set to its default value and disabled in Rel26. |

For more information on the parameters, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

- 
- 6 Click **OK**.

**Result:** The CRF Target table attributes are provisioned successfully.

END OF STEPS

# To provision a CRF Target List table

## Purpose

This procedure is used to provision a CRF Target List table.

## Description

Each CRF Target List has a list of CRF Targets or Target Groups.

## Steps to provision a CRF Target List table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → CRF Tables**.

**Result:** The **CRF Tables** window is displayed.

- 2 In the left pane, expand the **CRF Target List** folder.

**Result:** The CRF Target List tables are listed under the folder in the left pane.

If the folder is empty, add a CRF Target List table.

Perform the following steps in the **CRF Tables** window to add, rename, or delete a CRF Target List table :

| If you want to ...           | then ...  |
|------------------------------|---|
| add a CRF Target List table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...              | then ...   |
|---------------------------------|--|
| rename a CRF Target List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a CRF Target List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a CRF Target List table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the CRF Target List table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **CRF Tables** window to add, modify, or delete the CRF Target List table attributes:

| If you want to ...                        | then ...  |
|---|---|
| add the CRF Target List table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                         | then ...   |
|--|--|
| modify a CRF Target List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a CRF Target List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>              |

**5** Provision the following parameters:

| Parameter             | Description  |
|-----------------------|--|
| <b>Target List ID</b> | Range: 1 – 2048  |
| <b>Description</b>    | Up to 32 characters.   |
| <b>Target Type</b>    | Type 1/ Type 2<br>Default: Type 1  |
| <b>Location</b>       | Access (0) / Core (1)<br>Default: Core<br><b>Note:</b> For Type 2 , Location will be set to Core and the field will be disabled. |
| <b>Target List</b>    | Maximum of 100 Targets   |
| <b>Target Data</b>    |  |

| Parameter             | Description  |
|-----------------------|--|
| <b>Target ID</b>      | <p>Target IDs</p> <p><b>Note:</b> Target Index</p> <p>For Type 1: Only Access Targets are available if the List is set to Access and only Core targets are available if the List is set to Core location type.</p> <p>For Type 2: All the CRF Targets are available.</p> |
| <b>Transport Type</b> | <p>Any/SCTP/UDP/TCP/ TLS</p> <p>Default: UDP</p>   |
| <b>Order</b>          | <p>10/20</p> <p>Default: 10</p>  |
| <b>Priority</b>       | <p>10/20/30</p> <p>Default: 10</p>   |
| <b>Weight</b>         | <p>Range: 0 –100</p> <p>Default: 10</p>  |

For more information on the parameters, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

---

**6** Click **OK**.

**Result:** The CRF Target List table attributes are provisioned successfully.

END OF STEPS

---

# To provision a CRF Treatment table

## Purpose

This procedure is used to provision a CRF Treatment table.

## Steps to provision a CRF Treatment table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → CRF Tables**.

**Result:** The **CRF Tables** window is displayed.

- 2 In the left pane, expand the **CRF Treatment** folder.

**Result:** The CRF Treatment tables are listed under the folder in the left pane.

If the folder is empty, add a CRF Treatment table.

Perform the following steps in the **CRF Tables** window to add, rename, or delete a CRF Treatment table :

| If you want to ...            | then ...  |
|-------------------------------|---|
| add a CRF Treatment table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a CRF Treatment table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |

| If you want to ...            | then ...   |
|-------------------------------|--|
| delete a CRF Treatment table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a CRF Treatment table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the CRF Treatment table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **CRF Tables** window to add, modify, or delete the CRF Treatment table attributes:

| If you want to ...                       | then ...  |
|--|---|
| add the CRF Treatment table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.</li> </ol> <p><b>Result:</b> The <b>CRF Tables</b> window is displayed.</p> <ol style="list-style-type: none"> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a CRF Treatment table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.</li> </ol> <p><b>Result:</b> The <b>CRF Tables</b> window is displayed.</p> <ol style="list-style-type: none"> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                       | then ...  |
|--|---|
| delete a CRF Treatment table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter      | Description  |
|----------------|--|
| Treatment ID   | Range: 1 – 1024  |
| Description    | Up to 32 Characters  |
| Treatment Type | <ul style="list-style-type: none"> <li>Type 1 Target List</li> <li>Type 2 Target List</li> <li>Continue Re-Route</li> <li>Continue Task</li> <li>SIP Error Response</li> </ul> Default: Type 1 Target List |

| Parameter | Description  |
|-----------|--|
| Treatment | <p>The IDs displayed in this field depend on the Treatment Type selected.</p> <p>Type 1 – None , IDs of all Type 1 CRF Target Lists will be displayed</p> <p>Type 2 – None, IDs of all Type 2 CRF Target Lists will be displayed</p> <p>Continue Re-Route – None, CRF Route Plan IDs</p> <p>Continue Task – None, CRF Tasks IDs</p> <p>SIP Error Response – Default : 403 Forbidden</p> <ul style="list-style-type: none"><li>• 403 Forbidden (0)</li><li>• 404 Not Found (1)</li><li>• 480 Temporarily Not available (2)</li><li>• 488 Busy Here (3)</li><li>• 500 Internal Error (4)</li></ul> |

For more information on the parameters, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 6 Click **OK**.

**Result:** The CRF Treatment table attributes are provisioned successfully.

END OF STEPS

# To provision a CRF Digit Analysis Table

## Purpose

This procedure is used to provision a CRF Digit Analysis Table.

## Description

A maximum of 1 Million Digit Analysis entries are allowed across 1024 Digit Analysis tables.

## Steps to provision a CRF Digit Analysis Table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → CRF Tables**.

**Result:** The **CRF Tables** window is displayed.

- 2 In the left pane, expand the **CRF Digit Analysis Table** folder.

**Result:** The CRF Digit Analysis Table tables are listed under the folder in the left pane.

If the folder is empty, add a CRF Digit Analysis Table.

Perform the following steps in the **CRF Tables** window to add, rename, or delete a CRF Digit Analysis Table :

| If you want to ...              | then ...  |
|---------------------------------|---|
| add a CRF Digit Analysis Table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                 | then ...  |
|------------------------------------|---|
| rename a CRF Digit Analysis Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>     |
| delete a CRF Digit Analysis Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a CRF Digit Analysis Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the CRF Digit Analysis Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **CRF Tables** window to add, modify, or delete the CRF Digit Analysis Table attributes:

| If you want to ...                           | then ...  |
|--|---|
| add the CRF Digit Analysis Table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                            | then ...  |
|---|---|
| modify a CRF Digit Analysis Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol> |
| delete a CRF Digit Analysis Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.<br/><i>End of steps.</i></li> </ol>              |

**5** Provision the following parameters:

| Parameter                     | Description   |
|-------------------------------|---|
| <b>Digit String</b>           | String of a max 16 Characters   |
| <b>CRF Treatment Table ID</b> | None, IDs of the CRF Treatments provisioned in the CRF Treatment Table. |

For more information on the parameters, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

**6** Click **OK**.

**Result:** The CRF Digit Analysis Table attributes are provisioned successfully.

END OF STEPS

# To provision a CRF Trunk Group table

## Purpose

This procedure is used to provision a CRF Trunk Group table.

## Description

A maximum of 10,000 Trunk Group entries are allowed across 1024 Trunk Group tables.

## Steps to provision a CRF Trunk Group table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → CRF Tables**.

**Result:** The **CRF Tables** window is displayed.

- 2 In the left pane, expand the **CRF Trunk Group** folder.

**Result:** The CRF Trunk Group tables are listed under the folder in the left pane.

If the folder is empty, add a CRF Trunk Group table.

Perform the following steps in the **CRF Tables** window to add, rename, or delete a CRF Trunk Group table :

| If you want to ...           | then ...   |
|------------------------------|--|
| add a CRF Trunk Group table, | <ol style="list-style-type: none"><li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li><li>From the <b>Table Number</b> list, select the table number.</li><li>In the <b>Table Name</b> box, type a descriptive table name.</li><li>Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |

| If you want to ...              | then ...   |
|---------------------------------|--|
| rename a CRF Trunk Group table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a CRF Trunk Group table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a CRF Trunk Group table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.  
Add the CRF Trunk Group table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.
- 4 Perform the following steps at the **CRF Tables** window to add, modify, or delete the CRF Trunk Group table attributes:

| If you want to ...                        | then ...  |
|---|---|
| add the CRF Trunk Group table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                         | then ...  |
|--|---|
| modify a CRF Trunk Group table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol> |
| delete a CRF Trunk Group table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.<br/><i>End of steps.</i></li> </ol>              |

**5** Provision the following parameters:

| Parameter               | Description  |
|-------------------------|--|
| <b>Trunk Group</b>      | String of a max 256 Characters   |
| <b>Trunk Context</b>    | String of a max 256 Characters   |
| <b>CRF Treatment ID</b> | None, IDs of the CRF Treatments provisioned in the CRF Treatment Table |

For more information on the parameters, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

**6** Click **OK**.

**Result:** The CRF Trunk Group table attributes are provisioned successfully.

END OF STEPS

# To provision a CRF Route Plan table

## Purpose

This procedure is used to provision a CRF Route Plan table.

## Steps to provision a CRF Route Plan table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → CRF Tables**.

**Result:** The **CRF Tables** window is displayed.

- 2 In the left pane, expand the **CRF Route Plan** folder.

**Result:** The CRF Route Plan tables are listed under the folder in the left pane.

If the folder is empty, add a CRF Route Plan table.

Perform the following steps in the **CRF Tables** window to add, rename, or delete a CRF Route Plan table :

| If you want to ...             | then ...  |
|--------------------------------|---|
| add a CRF Route Plan table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a CRF Route Plan table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |

| If you want to ...             | then ...  |
|--------------------------------|---|
| delete a CRF Route Plan table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a CRF Route Plan table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the CRF Route Plan table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **CRF Tables** window to add, modify, or delete the CRF Route Plan table attributes:

| If you want to ...                        | then ...  |
|---|---|
| add the CRF Route Plan table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a CRF Route Plan table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                        | then ...  |
|---|---|
| delete a CRF Route Plan table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter                       | Description   |
|---------------------------------|---|
| <b>ID</b>                       | Range: 1 – 1024   |
| <b>Description</b>              | Up to 32 Characters   |
| <b>Route Plan Type</b>          | <ul style="list-style-type: none"> <li>Digit Analysis</li> <li>Trunk Group</li> </ul> <p>Default: Digit Analysis</p>  |
| <b>Type</b>                     | <ul style="list-style-type: none"> <li>Origination</li> <li>Destination</li> </ul> <p>Default: Destination</p>  |
| <b>Route Plan Data Table ID</b> | <p>None, IDs of the CRF DA Tables if Route Plan Type is set to Digit Analysis.</p> <p>None, IDs of the CRF Trunk Group Tables if Route Plan Type is set to Trunk Group.</p> |

Checks:

- If the **Route Plan Type** field on a given Route Plan is **Digit Analysis**, the Type has to be **Destination**.
- The **Route Plan Type** field on an already provisioned Route Plan is not allowed to be modified.

For more information on the parameters, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

6 Click **OK**.

**Result:** The CRF Route Plan table attributes are provisioned successfully.

END OF STEPS

# To provision a CRF Task Plan table

## Purpose

This procedure is used to provision a CRF Task Plan table.

## Steps to provision a CRF Task Plan table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → CRF Tables**.

**Result:** The **CRF Tables** window is displayed.

- 2 In the left pane, expand the **CRF Task Plan** folder.

**Result:** The CRF Task Plan tables are listed under the folder in the left pane.

If the folder is empty, add a CRF Task Plan table.

Perform the following steps in the **CRF Tables** window to add, rename, or delete a CRF Task Plan table :

| If you want to ...            | then ...  |
|-------------------------------|---|
| add a CRF Task Plan table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a CRF Task Plan table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |

| If you want to ...            | then ...   |
|-------------------------------|--|
| delete a CRF Task Plan table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a CRF Task Plan table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the CRF Task Plan table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **CRF Tables** window to add, modify, or delete the CRF Task Plan table attributes:

| If you want to ...                       | then ...  |
|--|---|
| add the CRF Task Plan table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a CRF Task Plan table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                       | then ...  |
|--|---|
| delete a CRF Task Plan table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter                 | Description  |
|---------------------------|--|
| <b>ID</b>                 | Range: 1 – 512   |
| <b>Description</b>        | Up to 32 Characters  |
| <b>Task Type</b>          | ENUM   |
| <b>Task Plan Data ID</b>  | IDs of the ENUM Profile(s)   |
| <b>Task Result</b>        | <ul style="list-style-type: none"> <li>ENUM success – E2U+sip</li> <li>ENUM success – E2U+pstn</li> <li>ENUM success – E2U+tel</li> <li>ENUM success – NXDOMAIN</li> <li>ENUM success – VOID</li> <li>ENUM failure</li> </ul> <p>Default: ENUM success – E2U+sip</p> |
| <b>Task Result Action</b> | <ul style="list-style-type: none"> <li>Continue Re-Route</li> <li>Next Route Plan</li> <li>Return to Application</li> </ul> <p>Default: Continue Re-Route</p>  |
| <b>Next Plan ID</b>       | IDs of the Route Plans or the Tasks  |

Checks:

- The **Task Type** field on an already provisioned Task is not allowed to be modified.

For more information on the parameters, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

**6 Click OK.**

**Result:** The CRF Task Plan table attributes are provisioned successfully.

.....  
E N D O F S T E P S .....

# To provision a CRF Route Priority List table

## Purpose

This procedure is used to provision a CRF Route Priority List table.

## Description

Each CRF Route Priority List entry has a list of a maximum of 8 Route Plans or Task Plans defined in CRF Route Plan table or the CRF Task plan table.

## Steps to provision a CRF Route Priority List table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → CRF Tables**.

**Result:** The **CRF Tables** window is displayed.

- 2 In the left pane, expand the **CRF Route Priority List** folder.

**Result:** The CRF Route Priority List tables are listed under the folder in the left pane.

If the folder is empty, add a CRF Route Priority List table.

Perform the following steps in the **CRF Tables** window to add, rename, or delete a CRF Route Priority List table :

| If you want to ...                   | then ...  |
|--------------------------------------|---|
| add a CRF Route Priority List table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                      | then ...   |
|---|--|
| rename a CRF Route Priority List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>          |
| delete a CRF Route Priority List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a CRF Route Priority List table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the CRF Route Priority List table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **CRF Tables** window to add, modify, or delete the CRF Route Priority List table attributes:

| If you want to ...                                | then ...  |
|---|---|
| add the CRF Route Priority List table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                                 | then ...   |
|--|--|
| modify a CRF Route Priority List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a CRF Route Priority List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>              |

**5** Provision the following parameters:

| Parameter  | Description  |
|--|--|
| <b>ID</b>  | Range: 1 – 2048  |
| <b>Description</b>   | Up to 32 Characters  |
| <b>Routing Priority List – Max of 8 Route or Task Plan IDs</b> |  |
| <b>Plan Type</b>   | Route or Task  |
| <b>Plan ID</b>   | Depending on whether the type selected is Route or Task, IDs of the entries provisioned in CRF Route Plan or the CRF Task Plan tables will be available. |

Checks:

- A given Route Plan ID can be used in a given list multiple times, but cannot appear in consecutive positions.
- A Route Priority List that is used by a CRF Route Profile in use on an IBC Route Profile will be allowed to point to only Route Plans of Digit Analysis Type.
- The last entry in a given Route Plan Priority List must be a Route Plan (not a Task).

For more information on the parameters, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

- 
- 6 Click OK.

**Result:** The CRF Route Priority List table attributes are provisioned successfully.

END OF STEPS

---

# To provision a CRF Route Profile table

## Purpose

This procedure is used to provision a CRF Route Profile table.

## Steps to provision a CRF Route Profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → CRF Tables**.

**Result:** The **CRF Tables** window is displayed.

- 2 In the left pane, expand the **CRF Route Profile** folder.

**Result:** The CRF Route Profile tables are listed under the folder in the left pane.

If the folder is empty, add a CRF Route Profile table.

Perform the following steps in the **CRF Tables** window to add, rename, or delete a CRF Route Profile table :

| If you want to ...                | then ...  |
|-----------------------------------|---|
| add a CRF Route Profile table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a CRF Route Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |

| If you want to ...                | then ...   |
|-----------------------------------|--|
| delete a CRF Route Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a CRF Route Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the CRF Route Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **CRF Tables** window to add, modify, or delete the CRF Route Profile table attributes:

| If you want to ...                           | then ...  |
|--|---|
| add the CRF Route Profile table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a CRF Route Profile table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>CRF Tables</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                           | then ...  |
|--|---|
| delete a CRF Route Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter                  | Description  |
|----------------------------|--|
| ID                         | Range: 1 – 2048  |
| Description                | Up to 32 Characters  |
| Route Priority List 1      | None – IDs of the CRF Route Priority Lists   |
| No Match Action for List 1 | <ul style="list-style-type: none"> <li>Return No Match</li> <li>Continue Next Route Priority List</li> </ul> <p>Default: Return No Match</p> |
| Route Priority List 2      | None – IDs of the CRF Route Priority Lists   |
| Spare ID                   | None – IDs of the Spare Table Records that are of CRF Route Profile type.  |

Checks:

- If the **No Match Action** field is set to *Continue Next Route Priority List*, the **Route Priority List 2** field must be populated with a valid value.

6 Click **OK**.

**Result:** The CRF Route Profile table attributes are provisioned successfully.

For more information on the parameters, see the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS





# 5 Manage services

## Overview

### Purpose

This chapter includes the procedures that are required to set up Alcatel-Lucent IP Session Control related services.

### Contents

|  |             |
|--|-------------|
| <b>To provision nomadic access</b>   | <b>5-6</b>  |
| To enable/disable nomadic user access                                      | 5-7         |
| <b>To provision the geographic location service for VoWLAN subscribers</b> | <b>5-8</b>  |
| To provision a MACaddress to Location table                                | 5-9         |
| To provision a Map Special Code to Dialed Number                           | 5-11        |
| To provision Geographic Location Server                                    | 5-13        |
| To provision client access to the Geographic Location Server               | 5-15        |
| <b>To provision multiple home domains</b>                                  | <b>5-17</b> |
| To provision multiple home domains   | 5-18        |
| <b>To provision IMS roaming</b>  | <b>5-20</b> |
| To provision IMS roaming   | 5-21        |
| <b>To provision SIP message screening</b>                                  | <b>5-22</b> |
| To provision an SIP Filter   | 5-23        |
| To provision an SIP Filter Header Rule                                     | 5-28        |
| To provision an SIP Filter Body Rule                                       | 5-36        |
| To provision an SIP Filter Reference Rule                                  | 5-44        |
| To provision an SIP Filter Parameter Rule                                  | 5-50        |
| To provision an SIP Filter Set   | 5-57        |

|  |              |
|--|--------------|
| <b>To provision priority mode</b>  | <b>5-60</b>  |
| To provision an Emergency Identifiers List   | 5-61         |
| To provision an NGN GETS Identifier List   | 5-64         |
| <b>To provision security gateway</b>   | <b>5-67</b>  |
| To provision an SIP Flow Trusted/Untrusted Rate Limit Rule Set                     | 5-68         |
| To provision an SIP Aggregate Trusted/Untrusted Rate Limit Rule Set                | 5-72         |
| To provision a Flow Source Address Policy  | 5-76         |
| To provision an Aggregate Source Address Policy                                    | 5-80         |
| To provision a Registration Failure Policy   | 5-83         |
| To provision an Application Layer Policy   | 5-87         |
| To provision a Security Gateway Profile  | 5-90         |
| <b>To provision support of digit analysis and normalization function</b>           | <b>5-94</b>  |
| Introduction to Digit Analysis (DA) tables   | 5-95         |
| Digit Analysis (DA) Rules  | 5-98         |
| Digit Analysis (DA) Rules -BGCF  | 5-105        |
| To provision a SIP Error Code table  | 5-106        |
| To provision an IMS Digit Table  | 5-110        |
| <b>To provision ICSI</b>   | <b>5-116</b> |
| To provision an ICSI profile   | 5-117        |
| <b>To provision bearer statistics collection on the iAGCF</b>                      | <b>5-122</b> |
| Support collecting Bearer statistics at AGCF from Access GW                        | 5-123        |
| <b>To provision the support of session and bandwidth limits per enterprise/PBX</b> | <b>5-124</b> |
| To provision a Virtual Group profile   | 5-125        |
| To provision a Service Level Policy  | 5-129        |
| To provision the IBC-A VG Policy   | 5-133        |
| To provision a VG and Service Mapping Profile                                      | 5-137        |
| <b>To provision signaling firewall</b>   | <b>5-141</b> |
| To provision FEPH Flow Policy  | 5-142        |
| Provision an Aggregate Packet Policy   | 5-147        |
| Provision an Aggregate Flow Policy   | 5-150        |
| Provisioning task flow for hardware acceleration                                   | 5-151        |
| Provision an Aggregate Policy Assignment   | 5-154        |

|  |              |
|--|--------------|
| To provision an IPsec Parameters table   | 5-155        |
| <b>Signaling Firewall configuration</b>  | <b>5-159</b> |
| External subnets   | 5-160        |
| Published NI IP addresses for FEPH and IMS services  | 5-161        |
| Default gateway and/or static routes for IMS services  | 5-162        |
| <b>IMS Service Growth with an existing FEPH Service</b>  | <b>5-163</b> |
| To grow an IMS service that is FEPH-enabled  | 5-164        |
| To disable FEPH on an FEPH-enabled IMS service   | 5-166        |
| To add FEPH IPv4 or IPv6 capability for an IMS service   | 5-167        |
| To remove FEPH IPv4 or IPv6 capability for an IMS service  | 5-170        |
| <b>Signaling Firewall Service Growth with existing IMS Services</b>  | <b>5-172</b> |
| Signaling Firewall growth preparation and planning   | 5-173        |
| To grow Signaling Firewall and FEPH on an existing network   | 5-179        |
| To grow Signaling Firewall and FEPH on a new network   | 5-191        |
| FEPH growth cleanup  | 5-200        |
| Service growth of FEPH service on HSPP4 of Malban (Hub) card   | 5-201        |
| fephGrowth command   | 5-208        |
| FEPH growth error-handling   | 5-211        |
| FEPH growth worksheet  | 5-212        |
| <b>Migration procedure for signaling firewall load balancer/distribution function</b>  | <b>5-222</b> |
| Migration Procedure for Signaling Firewall Load Balancer/Distribution Function   | 5-223        |
| <b>To provision signaling firewall load balancer or distribution function with single IP address exposed for the Gm interface to end users</b> | <b>5-229</b> |
| To provision a Published NI Group Assignment table   | 5-230        |
| <b>To provision common announcement module (CANM)</b>  | <b>5-235</b> |
| To provision a Treatment Trigger Data Table  | 5-236        |
| To provision a CANM Profile Table  | 5-239        |
| <b>To provision iAGCF support of network traffic management (NTM)</b>  | <b>5-245</b> |
| To provision an AGCF Cause Code To H248 Tone Table   | 5-246        |
| <b>To provision CMCC emergency service and P-CSCF SIP header manipulation</b>  | <b>5-249</b> |
| To provision an Access Location to ESRN Mapping Table  | 5-250        |

|   |              |
|---|--------------|
| To provision an IP Address Mapping Table  | 5-255        |
| To provision a Default Access Location Table  | 5-259        |
| <b>To provision support for sending offline charging data to the CCF provisioned to the CTS</b> | <b>5-263</b> |
| Support sending offline charging data to the CCF provisioned to the CTS                         | 5-264        |
| <b>To provision limit for TCP connections</b>   | <b>5-265</b> |
| To provision a Remote IP Policy Table   | 5-266        |
| <b>To provision IMUX services</b>   | <b>5-270</b> |
| To provision IMUX to IMS Association Table  | 5-271        |
| To provision IMUX port  | 5-274        |
| <b>To provision iHSS/iSLF support of per-enterprise domains</b>                                 | <b>5-279</b> |
| iHSS/iSLF support of per-enterprise domains   | 5-280        |
| Provisioning the Subscriber Home Domain Table   | 5-281        |
| <b>To provision MSRP peak data rate support to enhance user experience</b>                      | <b>5-285</b> |
| To provision an SDP Media MSRP Table  | 5-286        |
| <b>To provision access border for IMS or pre-IMS core</b>                                       | <b>5-289</b> |
| To provision IBC-A Profile  | 5-290        |
| To provision IBC Route Profile  | 5-297        |
| To provision Target Group Table   | 5-304        |
| To provision Target Group List  | 5-310        |
| To provision IBC Domain Table   | 5-314        |
| To provision Trunk Group  | 5-318        |
| To provision ACL List   | 5-322        |
| <b>To provision iAGCF line OOS and CPC display functionalities</b>                              | <b>5-327</b> |
| To provision an AGCF CPC String to CPC Digit Table  | 5-328        |
| <b>To provision Access Transfer Control Function (ATCF) support</b>                             | <b>5-331</b> |
| To provision an STN-SR Table  | 5-332        |
| <b>To provision SIP heartbeat after failure to reach a network element</b>                      | <b>5-336</b> |
| To provision an SIP Heartbeat after failure Exemption Table                                     | 5-337        |
| <b>Support Multiple Access Network Subnets on FEPH</b>  | <b>5-341</b> |
| Support multiple access network subnets on FEPH   | 5-342        |
| To grow a new external access subnet  | 5-343        |

|  |       |
|--|-------|
| To convert one ordinary subnet to external access subnet | 5-360 |
| To degrow one external access subnet                     | 5-371 |

# To provision nomadic access

## Overview

### Purpose

This section provides the procedure(s) to provision nomadic access.

### Contents

|                                       |     |
|---------------------------------------|-----|
| To enable/disable nomadic user access | 5-7 |
|---------------------------------------|-----|

## To enable/disable nomadic user access

### Purpose

This procedure is used to enable or disable the Block Nomadic User Access service.

### Procedure to enable/disable nomadic user access

Perform the following steps at the Provisioning GUI.

- 1 Select **IMS → IMS Components → SCSCF Tables..**

**Result:** The **SCSCF Tables** window is displayed.

- 2 Expand the **SCSCF Profile** folder.

Right-click the desired table that you want to open and select **Open** from the menu to open the table.

- 3 Select **Attributes → Modify Table Attributes** to modify the entry.

**Result:** The **SCSCF Profile Attributes** window is displayed.

- 4 On the **Registration** tab, select **Option to Block Nomadic User Access** to enable the Block Nomadic User Access service.

The Block Nomadic User Access feature restricts Consumer VoIP subscribers from registering with the IMS from another access network than their own pre-assigned Residential Gateway. By default the feature is disabled.

- 5 Select **OK** to save and close the window.

See “[To provision an S-CSCF profile](#)” (p. 4-15).

For more information about the parameters, refer to *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision the geographic location service for VoWLAN subscribers

## Overview

### Purpose

This section provides the procedure(s) to provision settings for dual mode subscribers.

### Contents

|  |      |
|--|------|
| To provision a MACaddress to Location table                  | 5-9  |
| To provision a Map Special Code to Dialed Number             | 5-11 |
| To provision Geographic Location Server                      | 5-13 |
| To provision client access to the Geographic Location Server | 5-15 |

# To provision a MACaddress to Location table

## Purpose

This procedure is used to map MACaddress to Location for use by the Location Server Database for Voice over Wireless Local Area Network (VoWLAN), also referred to as the Geographic Location Server (GLS). This feature provides an optional LCP resident database containing geographic information for WLAN access points.

## Steps to provision MACaddress to Location table attributes

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → GLS**.

**Result:** The **GLS Tables** window is displayed.

- 2 Expand the **Macaddress to Location** folder to expand the folder. Right-click the table that you want to open and select **OPEN** from the menu.

| 3 | If you want to           | Then  |
|---|--------------------------|---|
|   | Add table attributes,    | <p>On the <b>Attributes</b> menu, click <b>Add Table Attributes</b>. The <b>Macaddress to Location</b> window is displayed. Continue with <b>Step 4</b>.</p> <p><i>End of Steps</i></p>   |
|   | Modify table attributes, | <ul style="list-style-type: none"> <li>• In the right pane, click anywhere on the row of attributes that you want to modify</li> <li>• On the <b>Attributes</b> menu, click <b>Modify Table Attributes</b>. The <b>Macaddress to Location</b> window is displayed. Continue with <b>Step 4</b>.</li> </ul> <p><i>End of Steps</i></p> |
|   | Delete table attributes, | <ul style="list-style-type: none"> <li>• In the right pane, click anywhere on the row of attributes that you want to delete</li> <li>• On the <b>Attributes</b> menu, click <b>Delete Table Attributes</b></li> <li>• In the dialog box that is displayed, click <b>OK</b> to confirm.</li> </ul> <p><i>End of Steps</i></p>          |

- 
- 4 Enter/modify fields as desired.
- 

- 5 Click **OK** to confirm.

For the parameter information, refer to the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

---

END OF STEPS

---

# To provision a Map Special Code to Dialed Number

## Purpose

This procedure is used to map Special Code to Dialed Number entries for use by the Location Server Database for Voice over Wireless Local Area Network (VoWLAN), also referred to as the Geographic Location Server (GLS). This feature provides an optional LCP resident database containing geographic information for WLAN access points.

## Steps to provision the Map Special Code to Dialed Number table attributes

Perform the following at the Provisioning GUI.

- 1 Select **IMS → GLS**.

**Result:** The **GLS Tables** window is displayed.

- 2 Expand the **Map codes to Dialed Number** folder. Right-click the table that you want to open and select **Open** from the menu.

| 3 | If you want to           | Then  |
|---|--------------------------|---|
|   | Add table attributes,    | On the <b>Attributes</b> menu, click <b>Add Table Attributes</b> . The <b>Map codes to Dialed Number</b> window appears. Continue with <b>Step 4</b> .  |
|   | Modify table attributes, | <ul style="list-style-type: none"><li>In the right pane, click anywhere on the row of attributes that you want to modify</li><li>On the <b>Attributes</b> menu, click <b>Modify Table Attributes</b>. The <b>Map codes to Dialed Number</b> window appears. Continue with <b>Step 4</b>.</li></ul>      |
|   | Delete table attributes, | <ul style="list-style-type: none"><li>In the right pane, click anywhere on the row of attributes that you want to delete</li><li>On the <b>Attributes</b> menu, click <b>Delete Table Attributes</b>.</li><li>In the dialog box that appears, click <b>OK</b> to confirm.</li></ul> <i>End of Steps</i> |

- 4 Enter/modify fields as desired.

- 
- 5 Click **OK** to confirm.

For the parameter information, refer to *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

---

END OF STEPS

---

# To provision Geographic Location Server

## Purpose

This procedure is used to provision the Location Server Database for Voice over Wireless Local Area Network (VoWLAN), also referred to as the Geographic Location Server (GLS). This feature provides an optional LCP resident database containing geographic information for WLAN access points.

Provisioning of a GLS server is a growth operation. A local boot host pair with the GLS service must be grown into an office and then provisioned. Only one GLS should be grown into an IMS network. When these two steps are complete, the Gls port is configured.

## Steps to provision Geographic Location Server

The following procedure is used to grow local boot host pair with the GLS service into an office. Note that only one GLS should be grown into an IMS network. Perform the following steps at the Provisioning GUI.

- 
- 1 Select **IMS → GLS**.

**Result:** The **GLS Tables** window is displayed.

---

- 2 Expand the **Port** folder.

Right-click the desired table and select **Open** from the menu.

---

| 3 | If you want to           | Then   |
|---|--------------------------|--|
|   | Add table attributes,    | On the <b>Attributes</b> menu, click <b>Add Table Attributes</b> .<br>The <b>Gls Port</b> window is displayed. Continue with <b>Step 5</b> .   |
|   | Modify table attributes, | <ul style="list-style-type: none"> <li>• In the right pane, click anywhere on the row of attributes that you want to modify</li> <li>• On the <b>Attributes</b> menu, click <b>Modify Table Attributes</b>. The <b>Gls Port</b> window is displayed.<br/>Continue with <b>Step 5</b>.</li> </ul> |

| If you want to           | Then  |
|--------------------------|---|
| Delete table attributes, | <ul style="list-style-type: none"> <li>In the right pane, click anywhere on the row of attributes that you want to delete</li> <li>On the Attributes menu, click <b>Delete Table Attributes</b></li> <li>In the dialog box that is displayed, click <b>OK</b> to confirm.</li> </ul> <p><i>End of Steps</i></p> |

4 Ensure Port Type is **GIs**.

5 Enter/modify Port Name.

6 Enter or modify Port Number.

7 Click **OK** to confirm.

For more information about the parameters, refer to *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision client access to the Geographic Location Server

## Purpose

This procedure is used to provision client access to the Location Server Database for Voice over Wireless Local Area Network (VoWLAN), also referred to as the Geographic Location Server (GLS). This feature provides an optional LCP resident database containing geographic information for WLAN access points.

To provision client access to the GLS from an S-CSCF or STAS the connection information interface for GIs must be entered and the GIs protocol added to the diameter profile used by the component requiring GLS access.

## Steps to provision client access to the Geographic Location Server

Perform the following for the component requiring GLS access:

- 
- 1 Access the Diameter Application ID using **IMS → Parameters/Timers → Diameter Application ID**.

**Result:** The Diameter Application ID window is displayed.

- 
- 2 Select Application Type **GIs** and ensure that the Diameter Application ID field is set to **55555556** (default).

Click **OK** to confirm.

- 
- 3 Access the Diameter profile using **IMS → IMS Tables → IMS → General → Diameter Profile**.

- 
- 4 Highlight the table row desired and click **add** or **modify**.

**Result:** The Diameter Connection Interface window appears.

- 
- 5 Select Application Type **GIs** and configure the remaining fields as desired.

Click **OK** to confirm.

- 
- 6 Access Service to Diameter Mapping using **IMS → IMS Tables → IMS → General → Service to Diameter Mapping**.

**Result:** The Service to Diameter Mapping window appears.

- 
- 7 Set Service/Host type to **Gls**.
  - 8 Select Blade(s) from the list.
  - 9 Select Diameter Profile from the list.

Click **OK** to confirm.

For more information about the parameters, refer to *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

---

# To provision multiple home domains

## Overview

### Purpose

This section provides the procedure(s) to provision multiple home domains.

### Contents

|                                    |      |
|------------------------------------|------|
| To provision multiple home domains | 5-18 |
|------------------------------------|------|

# To provision multiple home domains

## Purpose

This procedure is used to enable multiple home domains.

## Before you begin

The HSS must be provisioned with TEL URI for every subscriber.

## Steps to provision multiple home domains

Perform the following steps at the Provisioning GUI.

- 
- 1 Select **IMS → IMS General Tables**.

**Result:** The **General** window is displayed.

---

- 2 Select **P-NAPTR Target URI** and provision the required URIs.

For example: **icsf-stdn.s123.alcatellucentlab.com**

---

- 3 Select **P-NAPTR Target Region** and provision the required regions with each region choosing an I-CSCF from the **PNAPTR target URI** list

For example the PNAPTR Region FQDN is **operator.com**

---

- 4 Select **Home Domain** and provision the required domains.

For example: **operator.com**

---

- 5 Select **IMS → IMS Parameters/Times → NGSS Parameters/Timers**.

**Result:** The **NGSS Parameters/Timers** window is displayed.

---

- 6 On the **NGSS Parameters/Timers** window:

- Choose **Default Home Domain**
- Check **Enable Multiple Home Domains**.

*Note:* If **Multiple Home Domain** is checked, then **Home I-CSCF** cannot be provisioned and the local zone domain cannot be provisioned as home domain.

7 Select IMS → IMS Components → ICSCF Tables → ICSCF Profile.

Check Change SIP URI to TEL URI

*Note:* This requires the HSS to be provisioned with TEL URI for every SUBSCRIBER.

END OF STEPS

# To provision IMS roaming

## Overview

### Purpose

This section provides the procedure(s) to provision IMS roaming.

### Contents

|                          |      |
|--------------------------|------|
| To provision IMS roaming | 5-21 |
|--------------------------|------|

# To provision IMS roaming

## Purpose

This procedure is used to provision IMS roaming.

## Before you begin

It is assumed that the external DNS server that provides the URI for the entry point for a given external domain using NAPTR records is already provisioned.

## Steps to provision IMS roaming

Perform the following steps at the Provisioning GUI.

- 
- 1 Select **IMS → IMS Tables → IMS → General**.

**Result:** The **General** window is displayed.

---

- 2 Select **External Domain Routing** and provision the **Network Identifier** for the required external domains. In the Visited Network, roaming is supported for only those domains that are provisioned.

See , “[To provision an External Domain Routing table](#)” (p. 10-99).

---

- 3 Select **IMS → IMS Parameters/Timers → NGSS Parameters/Timers**.

**Result:** The **NGSS Parameters/Timers** window is displayed.

---

- 4 On the **NGSS Parameters/Timers** window:

- Provision **Default IBCF**

**Note:** For an external domain, if **Next Hop** is provisioned on **External Domain Routing** then the P-CSCF/S-CSCF/BGCF will use this for routing messages to that domain. Otherwise the **Default IBCF** from **NGSS Parameters/Timers** window will be used.

END OF STEPS

---

# To provision SIP message screening

## Overview

### Purpose

This section provides the procedure to provision SIP Message Screening.

### Contents

|   |      |
|---|------|
| To provision an SIP Filter                | 5-23 |
| To provision an SIP Filter Header Rule    | 5-28 |
| To provision an SIP Filter Body Rule      | 5-36 |
| To provision an SIP Filter Reference Rule | 5-44 |
| To provision an SIP Filter Parameter Rule | 5-50 |
| To provision an SIP Filter Set            | 5-57 |

# To provision an SIP Filter

## Purpose

This procedure is used to provision an SIP Filter.

## Description

The purpose of creating an SIP Filter is to define the Direction Rule (DR) and Message Rule (MR). For more information, see the topic "*SIP Message Screening*" in the *ISC Application User Guide*.

## Before you begin

### Points to remember:

- Each SIP Filter can support
  - One DR and one MR
  - Five Header Rules
  - Twenty-five Parameter Rules that is, five PRs per HR.
  - Ten Body Rules
  - Ten Reference Rules

**Note :** The execution order of the BRs, RRs, HRs and PRs can be modified after the rules have been created. The BR and RR are at the same level of execution as the HRs. The BRs, RRs and HRs can be created in any order of execution. However, there cannot be a BR or RR in between the HR and PR.

While creating the HRs and PRs, it is logical to create one HR at a time and the associated PRs first and then move to the next HR. However, this is not mandatory. All the HRs can be created first and then the PRs. The only sequence enforced is that the FR must be created before the HR and the HR before the PR. After the Filters are created they are assigned to a Filter Set. The Filter Set is assigned to the profile of the (CF) component (IBCF and/or P-CSCF).

- The number of filters that can be configured if the memory required does not exceed IMS service available configuration data is 2000.

## Steps to provision an SIP Filter table

Perform the following steps at the Provisioning GUI.

- 
- 1 Select **IMS → SIP Tables**.

**Result:** The **SIP Tables** window is displayed.

In the left pane, expand the **SIP Filter** folder.

**Result:** The SIP Filter tables are listed under the folder in the left pane.

If the folder is empty, add an SIP Filter table.

- 2 Perform the following steps in the **SIP Tables** window to add, rename, or delete an SIP Filter table:

| If you want to...           | Then...   |
|-----------------------------|---|
| add an SIP Filter table,    | <ol style="list-style-type: none"> <li>Right-click <b>SIP Filter</b> and select <b>Add Table</b>.</li> <li>Provide a <b>Table Number</b> and a <b>Table Name</b> in the <b>Add SIP Filter table</b> window that is displayed.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p>  |
| rename an SIP Filter table, | <ol style="list-style-type: none"> <li>Select the table you want to modify.</li> <li>Right-click and select <b>Rename Table</b></li> <li>Modify the table name in the <b>Rename SIP Filter table</b> window that is displayed and click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p>   |
| delete an SIP Filter table, | <ol style="list-style-type: none"> <li>Select the table you want to delete.</li> <li>Right-click and select <b>Delete Table</b>.</li> <li>Click <b>OK</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> <p><b>Note:</b> Before deleting, ensure that the SIP Filter table does not contain any records (that is, Filters) and the filter is disabled.</p> |

- 3 Double-click the desired SIP Filter table. The SIP Filter table opens in the right pane. Perform the following steps to add, modify, or delete the SIP Filter table attributes:

| If you want to ...               | Then ...   |
|----------------------------------|--|
| add SIP Filter table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Filter</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol> |

| If you want to ...                  | Then ...   |
|-------------------------------------|--|
| modify SIP Filter table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The SIP Filter window is displayed.</li> <li>3. Continue with <a href="#">Step 4</a> to provision the parameters.<br/><br/><b>Note:</b> The filter should be disabled before modifying the filter attributes.</li> </ol>                      |
| delete SIP Filter table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> <p><b>Note:</b> The filter should be disabled before deleting the filter attributes.</p> |

**4 Provision the following parameters:**

| Parameter   | Value   |
|---|---|
| <b>Filter ID</b>                                  | Enter a unique ID for the FR.   |
| <b>Description</b>                                | Enter the description of the FR.  |
| <b>Enable Filter</b>                              | <b>Enable or Disable</b> the FR.<br><br><b>Note:</b> The Filter should be disabled while provisioning the rules.  |
| <b>Direction</b>                                  | Select the message direction, whether <b>Inbound</b> or <b>Outbound</b> or <b>Both</b> .  |
| <b>Available SIP Methods/Filtered SIP Methods</b> | Use <b>Add</b> and <b>Delete</b> to assign <b>Filtered SIP Methods</b> from <b>Available SIP Methods</b> .  |
| <b>Other Method String</b>                        | Enter the method that needs to be filtered.<br><br><b>Note:</b> <ul style="list-style-type: none"> <li>• This parameter is available only if <b>Other</b> is selected in the <b>Filtered SIP Methods</b>.</li> <li>• At least one method must be entered either in <b>SIP Methods</b> or in <b>Other Method String</b>.</li> <li>• Use this option only if the available methods cannot be used.</li> </ul> |

| Parameter                    | Value  |
|------------------------------|--|
| <b>Method Negation</b>       | If <b>Method Negation</b> is set to <b>Yes</b> , the selected method(s) are excluded and the SIP Filter is applied to all other methods.   |
| <b>Message Type</b>          | Select whether the filter applies to <b>Request</b> , <b>Response</b> or <b>Both</b> .   |
| <b>Response Code</b>         | Enter response codes.<br><br>Response Code can be <b>All</b> , or in the <b>NNN</b> , <b>NNX</b> , <b>NXX</b> format where the first N can range from 1-6 and subsequentNs from 0 - 9. For example, 2xx, 201, 404, 4xx, and so on.   |
| <b>Action</b>                | Select an action type.<br><br>The following are the available values: <ul style="list-style-type: none"> <li>• <b>Discard</b> - To drop message and return.</li> <li>• <b>Modify</b> - To change response code.</li> <li>• <b>No action</b> - To continue with HR (if assigned).</li> <li>• <b>Reject</b> - To reject request with new response and continue with HRs (if assigned).</li> </ul> <p><b>Note:</b> The actions are restricted depending on the direction of the message. For more information, see the topic "<i>SIP Message Screening</i>" in the <i>ISC Application User Guide</i>.</p> |
| <b>New Response Code</b>     | Enter a string of maximum of 3 characters length in the format <b>NNN</b> , where the corresponding ranges are <b>(1 - 6)</b> <b>(0 - 9)</b> <b>(0 - 9)</b> .<br><br><b>New Response Code</b> is provisioned for the following reasons: <ul style="list-style-type: none"> <li>• To modify a message response when the <b>Action</b> is set to <b>Modify</b>.</li> <li>• To reject a message request when the <b>Action</b> is set to <b>Reject</b>.</li> </ul> Example: 404.  |
| <b>Reason Phrase</b>         | Enter the reason for the response.   |
| <b>SIP Message Size &gt;</b> | Enter the value of the SIP message size.<br><br>This specifies the expected maximum message size. The size can be imposed on incoming messages, outgoing messages, or messages in both directions.<br><br>This condition is true if the size of the message exceeds the size specified in this parameter. This condition is evaluated in conjunction with other MR conditions.   |

| Parameter                | Value  |
|--------------------------|--|
| HBR Rule Execution Order | <p>Use <b>Up</b> and <b>Down</b> to set the order of HR execution. This can be done after the HR is created or updated. The default order is set to the creation order of the HRs.</p> <p>The <b>Header Rule Execution Order</b> includes both <b>Rule Type</b> and <b>Rule ID</b>.</p> <p>The <b>Rule ID</b> ranges for the BR, HR, and RR are as follows:</p> <ul style="list-style-type: none"><li>• BR: 1 to 10</li><li>• HR: 1 to 5</li><li>• RR: 1 to 10</li></ul> <p>For information on HR, refer “<a href="#">To provision an SIP Filter Header Rule</a>” (p. 5-28).</p> |

**Note:** SIP Filter table contains both Direction Rule (DR) and Message Rule (MR).

5 Click **OK**.

**Result:** The SIP Filter is added or modified.

For more information on the parameters, see the topic “SIP Filter” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379..

END OF STEPS

# To provision an SIP Filter Header Rule

## Purpose

This procedure is used to provision an SIP Filter Header Rule.

## Description

The purpose of creating an SIP Filter Header Rule is to define the header rules. For more information, see the topic, "*SIP Message Screening*" in the *ISC Application User Guide*.

## Before you begin

### Points to remember:

- Ensure that the SIP Filters are provisioned and disabled.
- Each SIP Filter can only support five SIP Filter Header Rules.
- Each SIP Filter Header Rule can only support five SIP Parameter Rules.

## Steps to provision an SIP Filter Header Rule table

Perform the following steps at the Provisioning GUI:

**1** Select **IMS → SIP Tables**.

**Result:** The **SIP Tables** window is displayed.

In the left pane, expand the **SIP Filter Header Rule** folder.

**Result:** The SIP Filter Header Rule tables are listed under the folder in the left pane.

If the folder is empty, add an SIP Filter Header Rule table.

**2** Perform the following steps in the **SIP Tables** window to add, rename, or delete an SIP Filter Header Rule table:

| If you want to...                    | Then...   |
|--------------------------------------|---|
| add an SIP Filter Header Rule table, | <ol style="list-style-type: none"> <li>1. Right-click <b>SIP Filter Header Rule</b> and select <b>Add Table</b>.</li> <li>2. Provide a <b>Table Number</b> and a <b>Table Name</b> in the <b>Add SIP Filter Header Rule table</b> window that is displayed.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |

| If you want to...                       | Then...  |
|---|--|
| rename an SIP Filter Header Rule table, | <ol style="list-style-type: none"> <li>1. Select the table you want to modify.</li> <li>2. Right-click and select <b>Rename Table</b></li> <li>3. Modify the table name in the <b>Rename SIP Filter Header Rule table</b> window that is displayed and click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p>   |
| delete an SIP Filter Header Rule table, | <ol style="list-style-type: none"> <li>1. Select the table you want to delete.</li> <li>2. Right-click and select <b>Delete Table</b>.</li> <li>3. Click <b>OK</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> <p><b>Note:</b> Before deleting, ensure that the SIP Filter Header Rule table does not contain any records (that is, Filters) and the filter is disabled.</p> |

- 3 Double-click the desired SIP Filter Header Rule table. The SIP Filter Header Rule table opens in the right pane. Perform the following steps to add, modify, or delete the SIP Filter Header Rule table attributes:

| If you want to ...                              | Then ...   |
|---|--|
| add SIP Filter Header Rule table attributes,    | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Filter Header Rule</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>   |
| modify SIP Filter Header Rule table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Filter Header Rule</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol> |

| If you want to ...                              | Then ...  |
|---|---|
| delete SIP Filter Header Rule table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> <p><b>Note:</b> Before deleting the Header Rule table attributes, remove the parameters associated with the HR. See “<a href="#">To provision an SIP Filter Parameter Rule</a>” (p. 5-50).</p> |

**4** Provision the following parameters:

**Note:**

- While provisioning the SIP Filter Header Rule, the associated SIP Filter must be disabled.
- The **Conditions Fields** are used to specify the criteria that needs to be met to execute the action and/or the PR.
- The **Actions Fields** can be executed only if the results of the conditions are *true*.
- Depending on the action, only certain parameters are provisioned.

| Parameter             | Description  |
|-----------------------|--|
| <b>Filter ID</b>      | Enter the filter ID that you want to associate with this Header rule.  |
| <b>Header ID</b>      | Select a unique header ID for the HR. The available values are 1 to 5.<br><b>Note:</b> Each SIP Filter can support only five HRs.  |
| <b>Description</b>    | Enter the description of the header rule.  |
| <b>Case Sensitive</b> | <p>The following two options are available:</p> <ul style="list-style-type: none"> <li>Choose <b>Yes</b> to select case sensitive.</li> <li>Choose <b>No</b> to select case insensitive.</li> <li>The default value is <b>No</b>.</li> </ul> <p>This parameter specifies if this rule applies case sensitive or case insensitive character processing for the content of the identified header. This parameter applies to the condition and action of this rule.</p> |

| Parameter                 | Description   |
|---------------------------|---|
| <b>Condition Fields</b>   |   |
| <b>Form</b>               | Select the position in the SIP message to apply the rule. The options available are: <ul style="list-style-type: none"> <li>• <b>Request URI</b></li> <li>• <b>Header</b></li> <li>• <b>Response Code</b></li> </ul>  |
| <b>Header Name</b>        | This parameter is enabled only if the form is set to Header. The parameter is populated with the Header name this rule applies to.  |
| <b>Regular Expression</b> | <p>Enter regular expressions to match and analyze the content of the Header or Request URI and Content type (content: media-type and parameters).</p> <p>It is used to determine if a pattern exists in the content of the form (header content, request URI). For example, use a RegEx to determine if the content contains a digit string <code>.*(911).*</code>.</p> <p>Backref reference can be accessed in the rule. The syntax for the condition regular expression is <code>\c1-\c9</code>. For example <code>\c3</code>. Where “c” identifies the backref as a condition regular expression backref.</p> <p><b>Note:</b> RegExp allows more than nine references in a RegExp condition. However, only the first nine references can be referenced using <code>\c1-\c9</code> in other parameters in that Header Rule.</p> |

| Parameter                    | Description   |
|------------------------------|---|
| <b>Boolean Condition</b>     | <p>Enter a logical Boolean expression using the BR base condition and the results of previous rule conditions. The BR base condition is defined by the previous condition fields in the present BR. The HR or PRs can be reference by H and ID number and P and ID number respectively.</p> <p>The parameter supports basic boolean operator symbols, “&amp;” (and), “ ” (or), “!” (not), and parentheses (to specify preference).</p> <p>A few examples (in B4):</p> <ul style="list-style-type: none"> <li>• B4 &amp; (! (H2   H3)) - This means that the condition is met if the base BR condition (B4) is true and neither of the conditions H2 or H3 are true.</li> <li>• !B4 - Applies negation to the BR base condition.</li> <li>• (H1&amp;P1) (H2 &amp;(!H3)) - This means that the condition is met if the result of (H1&amp;P1) or (H2&amp;(!H3)) is true.</li> </ul> <p>The result of the Boolean evaluation indicates if the action is performed or not.</p> |
| <b>SIP Message Size &gt;</b> | <p>Enter an integer value between 0 and 25,000,000.</p> <p>This parameter specifies the expected maximum message size. This condition is true if the size of the message exceeds the size specified in this parameter. This condition is evaluated in conjunction with other HR conditions.</p>   |
| <b>Occurrence</b>            | <p>Select the number of headers in the list to which this rule is applied. The default value is 1.</p> <p>This parameter is used to manipulate the list headers and it depends on the <b>Action</b> parameter value. For more information, see the topic, <i>"SIP Message Screening" in the ISC Application User Guide</i>.</p>   |

| Parameter            | Description   |
|----------------------|---|
| Compare              | <p>This parameter provides the ability to compare strings for example, string1 and string2.</p> <p>The following list gives the possible values for the argument passed in to the Compare Reference:</p> <ul style="list-style-type: none"> <li>• Reference to a previously saved Rule in that Filter (H1-5, B1-10, R1-10, or P1-25)</li> <li>• Backref from the Conditional fields Regular Expression from that Rule (<code>\c{1-9}</code>)</li> <li>• Keyword value, for example, <code>\$SRIP\$</code>, <code>\$SRPRT\$</code>, and so on</li> </ul> <p>For more information on keyword functionality, see the topic, "<i>SIP Message Screening</i>" in the <i>ISC Application User Guide</i>.</p> <ul style="list-style-type: none"> <li>• Fixed string</li> </ul> <p><b>Note:</b> If any of the reference is empty, the condition is always true.</p> <p>String1 and string2 can be compared based on:</p> <ul style="list-style-type: none"> <li>• Equal (for example, <math>S_1 = S_2</math>)</li> <li>• Subset (for example, <math>S_1 \subseteq S_2</math>)</li> <li>• Superset (for example, <math>S_2 \supseteq S_1</math>)</li> </ul> |
| <b>Action Fields</b> |   |
| Action               | <p>Select an action type.</p> <p>The following are the available values:</p> <ul style="list-style-type: none"> <li>• <b>Add</b> - To add a new header only.</li> <li>• <b>Discard</b> - To discard the message.</li> <li>• <b>Modify</b> - To change content of the Header or REQ-URI and to remove content of the Header.</li> <li>• <b>No action</b> - To continue with the PR or next HR.</li> <li>• <b>Reject</b> - To reject the request with the specified response code.</li> <li>• <b>Remove</b> - To delete the header and or message Body.</li> <li>• <b>Save</b> - To save the content of the header or Update String.</li> </ul> <p><b>Note:</b> The actions are restricted depending on the direction of the message. For more information, see the topic, "<i>SIP Message Screening</i>" in the <i>ISC Application User Guide</i>.</p>   |
| New Header Name      | Enter the name of the new header that needs to be added.  |

| Parameter                   | Description  |
|-----------------------------|--|
| <b>Update String</b>        | <p><b>Update String</b> values can be a combination of the following elements:</p> <ul style="list-style-type: none"> <li>• A text string enclosed by double quotes (for example, “abcd”).</li> <li>• Backrefs for referencing strings in the action field <b>RegularExpression</b> parameter. Valid format for backrefs is \a1 – \a9.</li> <li>• Backrefs for referencing strings in the condition field <b>RegularExpression</b> parameter. Valid format for backrefs is \c1 – \c9.</li> <li>• References to information saved by previous rule action (H1-H5, P1-P25, B1-B10, R1-R10).</li> <li>• A keyword value, for example, \$SRIP\$, \$SRPRT\$, and so on.</li> </ul> <p>For more information on keyword functionality, see the topic, <i>"SIP Message Screening" in the ISC Application User Guide</i>.</p> |
| <b>Reg Ex Source Buffer</b> | <p>This parameter is used by the <b>Regular Expression</b> parameter to apply the regular expression specified. If the regular expression is not specified then it uses the content of the current HR.</p> <p>This parameter supports .</p> <p>This parameter can contain one of the following:</p> <ul style="list-style-type: none"> <li>• H1-H5, B1-B10, R1-R10, P1-P25</li> <li>• \c1-\c9</li> <li>• Keyword reference, for example, \$SRIP\$, \$SRPRT\$, and so on</li> </ul> <p>For more information on keyword functionality, see the topic, <i>"SIP Message Screening" in the ISC Application User Guide</i>.</p>  |

| Parameter                             | Description   |
|---------------------------------------|---|
| <b>Regular Expression</b>             | <p>Enter regular expressions to analyze the content of the Header, Request URI or Content Type header.</p> <p>The result of this parameter that is, backref format is used by the Update String to modify the specified Form content or by the HR to save the value (or part of the value) in the Update String.</p> <p>If specific content needs to be saved, then the Update String and the Regular Expression can be used simultaneously. The save operation is executed only if the return of the RegEx is a match.</p> <p>For example, to save only the IP address content (IPV4) of the header, enter <b>Regular Expression</b> = <code>([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}):([0-9]{1,4})</code> and the backref in the <b>Update String</b> = <code>\1</code>.</p> <p>The action backref syntax, changes from <code>\1-9</code> to <code>\a1-9</code>.</p> |
| <b>Response Code</b>                  | <p>Enter a value between 400 – 699 or a Null String.</p> <p>For example: 404. This parameter is enabled only when the <b>Action</b> is set to <i>Reject</i>.</p>  |
| <b>Reason Phrase</b>                  | Enter the reason for the new response.  |
| <b>Parameter Rule Execution Order</b> | <p>Use <b>Up</b> and <b>Down</b> to set the order of PR execution.</p> <p>This can be done after the PRs are created or updated. The default order is set to the creation order of the PRs.</p> <p>For information on PR, see “<a href="#">To provision an SIP Filter Parameter Rule</a>” (p. 5-50).</p>  |

5 Click **OK**.

**Result:** The SIP Filter Header Rule is added or modified.

For more information about the parameters, see the topic “SIP Filter Header Rule” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision an SIP Filter Body Rule

## Purpose

This procedure is used to provision an SIP Filter Body Rule.

## Description

The Body Rule (BR) provides the capability to retrieve and manipulate the body content in the SIP message.

The purpose of creating an SIP Filter Body Rule is to define the body rules. For more information, see the topic, "*SIP Message Screening*" in the *ISC Application User Guide*.

## Before you begin

### Points to remember:

- Ensure that the SIP Filters are provisioned and disabled
- Each SIP Filter can support only ten SIP Filter Body Rules

## Steps to provision an SIP Filter Body Rule table

Perform the following steps at the Provisioning GUI:

**1** Select **IMS → SIP Tables**.

**Result:** The **SIP Tables** window is displayed.

In the left pane, expand the **SIP Filter Body Rule** folder.

**Result:** The SIP Filter Body Rule tables are listed under the folder in the left pane.

If the folder is empty, add an SIP Filter Body Rule table.

**2** Perform the following steps in the **SIP Tables** window to add, rename, or delete an SIP Filter Body Rule table:

| If you want to...                  | Then...   |
|------------------------------------|---|
| add an SIP Filter Body Rule table, | <ol style="list-style-type: none"> <li>1. Right-click <b>SIP Filter Body Rule</b> and select <b>Add Table</b>.</li> <li>2. Provide a <b>Table Number</b> and a <b>Table Name</b> in the <b>Add SIP Filter Body Rule table</b> window that is displayed.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |

| If you want to...                     | Then...   |
|---------------------------------------|---|
| rename an SIP Filter Body Rule table, | <ol style="list-style-type: none"> <li>Select the table you want to modify.</li> <li>Right-click and select <b>Rename Table</b></li> <li>Modify the table name in the <b>Rename SIP Filter Body Rule table</b> window that is displayed and click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |
| delete an SIP Filter Body Rule table, | <ol style="list-style-type: none"> <li>Select the table you want to delete.</li> <li>Right-click and select <b>Delete Table</b>.</li> <li>Click <b>OK</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>   |

- 3 Double-click the desired SIP Filter Body Rule table. The SIP Filter Body Rule table opens in the right pane. Perform the following steps to add, modify, or delete the SIP Filter Body Rule table attributes:

| If you want to ...                            | Then ...   |
|---|--|
| add SIP Filter Body Rule table attributes,    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Filter Body Rule</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>   |
| modify SIP Filter Body Rule table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Filter Body Rule</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>        |
| delete SIP Filter Body Rule table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> |

- 4 Provision the following parameters:

**Note:**

- While provisioning the SIP Filter Body Rule, the associated SIP Filter must be disabled.
- The **Conditions Fields** are used to specify the criteria that needs to be met to execute the action.
- The **Actions Fields** can be executed only if the result of the conditions are *true*.
- Depending on the action, only certain parameters are provisioned.

| Parameter               | Description  |
|-------------------------|--|
| <b>Filter ID</b>        | Select the filter ID that you want to associate with this Body rule.   |
| <b>Body Rule ID</b>     | Select a unique Rule ID for the BR. The available values are 1 to 10.<br><br><b>Note:</b> Each SIP Filter can support only ten BRs.  |
| <b>Description</b>      | Enter the description of the Body rule.  |
| <b>Case Sensitive</b>   | Specify if this rule applies to case sensitive ( <b>Yes</b> ) or case insensitive ( <b>No</b> ) character processing for content information.  |
| <b>Condition Fields</b> |  |
| <b>Form</b>             | <p>This parameter specifies the manner in which BR rule is applied in the SIP message.</p> <p>Select from the following available options:</p> <ul style="list-style-type: none"> <li>• <i>Body</i> - The content of the content type specified by the media is analyzed.</li> <li>• <i>Body Content</i> - The content of the body (sdp) can be manipulated.</li> </ul> <p>When <b>Form</b> is set to <i>Body</i>: The content is analyzed based on the specified media type and matching Content-Type headers. This is needed for multipart bodies when Content indirection is expected. For example, BR searches for message or external-body and can analyze the entire content of the header for a specific URL.</p> |
| <b>Content Type</b>     | <p>This parameter specifies the following:</p> <ul style="list-style-type: none"> <li>• Media type expected in the Content Type header.</li> <li>• Type of body attachments that accept the BR rule.</li> </ul> <p>When <b>Form</b> = <i>Body content</i>, any media type can be entered .</p> <p>When <b>Form</b> = <i>Body</i>, the content type can be entered or left blank. When left blank this indicates that the rule is checking if the message contains a body.</p>  |

| Parameter                 | Description   |
|---------------------------|---|
| <b>Regular Expression</b> | <p>Enter the regular expression to evaluate the contents of the identified body attachment(s).</p> <p><b>Note:</b> RegExp allows more than nine references in a RegExp condition. However, only the first nine references can be referenced using \c1-c9 by other BR fields.</p>  |
| <b>Boolean Condition</b>  | <p>Enter a logical Boolean expression using the BR base condition and the results of previous rule conditions.</p> <p>The BR base condition is defined by the previous condition parameters in the present BR.</p> <p>The basic boolean operator symbols, “&amp;” (and), “ ”(or), “!” (not), parenthesis (to specify preference) are supported.</p> <p>A few examples (in B4):</p> <ul style="list-style-type: none"> <li>• B4 &amp; (! (H2   H3)) - This means that the condition is met if the base BR condition (B4) is true and neither of the conditions H2 or H3 are true.</li> <li>• !B4 applies negation to the BR base condition.</li> </ul> |
| <b>Body Size &gt;</b>     | <p>Enter the maximum content length allowed in the SIP message body. This applies to Content Type.</p> <p>The condition is true when the body of a message exceeds this length. This parameter applies to single-part bodies or multi-part bodies.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• When <b>Form</b> = <i>Body Content</i>, the values are 0-250000, where zero indicates not set.</li> <li>• When <b>Form</b> = <i>Body</i>, blank or 0 – 250000 can be selected.</li> </ul>   |
| <b>Occurrence</b>         | <p>When Form = <i>Body</i>, Action = Remove, then, <b>Occurrence</b> can be set to 1-10 or All. The default value is 1.</p> <p>This allows the rule to remove multiple bodies of the same media type.</p>   |

| Parameter            | Description   |
|----------------------|---|
| Compare              | <p>This parameter provides the ability to compare strings for example, string1 and string2.</p> <p>The following list gives the possible values for the argument passed in to the Compare Reference:</p> <ul style="list-style-type: none"> <li>• Reference to a previously saved Rule in that Filter (H1-5, B1-10, R1-10, or P1-25)</li> <li>• Backref from the Conditional Fields Regular Expression from that Rule (<code>\c{1-9}</code>)</li> <li>• Keyword reference, for example, <code>\$SRIP\$</code>, <code>\$SRPRT\$</code>, and so on<br/>For more information on keyword function, see the topic, <i>"SIP Message Screening" in the ISC Application User Guide</i>.</li> <li>• Fixed string</li> </ul> <p>String1 and string2 can be compared based on:</p> <ul style="list-style-type: none"> <li>• Equal (for example, <math>S1 = S2</math>)</li> <li>• Subset (for example, <math>S1 \subseteq S2</math>)</li> <li>• Superset (for example, <math>S2 \supseteq S1</math>)</li> </ul> |
| <b>Action Fields</b> |   |

| Parameter  | Description  |
|------------|--|
| Action     | <p>Select an action type from the following options:</p> <ul style="list-style-type: none"> <li>• <b>Add</b> - To add a new header if <b>Form</b> is set to <i>Body</i> and all the other conditions are met. This action does not apply if <b>Form</b> is set to <i>Body Content</i>.</li> <li>• <b>Discard</b> - To drop messages received with a body that meets the specified BR conditions.</li> <li>• <b>Modify</b> - To modify the content of a body attachment.</li> <li>• <b>No Action</b> - Only conditional processing is done to the body. This is the default value.</li> <li>• <b>Reject</b> - To reject requests received with a body that meets the specified HR conditions. Request is rejected by returning the response specified in the BR rule.</li> <li>• <b>Remove</b> - To remove a body from the message.</li> <li>• <b>Replace</b> - To replace the content of a body attachment without retrieving a copy of the body received. This action is useful when multiple rules are used to manipulate a body. For example, the “save” action saves a copy of the body and RRs are used to analyze and manipulate the saved information. “Replace” can then be used to replace the content of the body with the saved or modified information.</li> <li>• <b>Save</b> - To save the content of the body specified in the condition. The saved information is stored in the memory for the use of another rule in the same SIP Filter. Saved information is kept until all the rules in the SIP Filter have been processed.</li> </ul> <p>The default value is <i>No Action</i>.</p> |
| New Header | Enter a new header name between 0 – 50.  |

| Parameter                   | Description  |
|-----------------------------|--|
| <b>Update String</b>        | <p>Enter the value that will be used when the BR <b>Action</b> is set to <b>Modify</b>, <b>Save</b> and <b>Replace</b>. For <b>Modify</b> the content of the body is replaced with the content of this parameter. For <b>Save</b>, the content of the body or the content of this parameter is saved.</p> <p><b>Update String</b> values can be a combination of the following elements:</p> <ul style="list-style-type: none"> <li>• A text string enclosed by double quotes (for example, “abcd”).</li> <li>• Backrefs for referencing strings in the action field <b>RegularExpression</b> parameter. Valid format for backrefs is \a1 – \a9.</li> <li>• Backrefs for referencing strings in the condition field <b>RegularExpression</b> parameter. Valid format for backrefs is \c1 – \c9.</li> <li>• References to information saved by previous rule action (H1-H5, P1-P25, B1-B10, R1-R10).</li> <li>• A keyword value, for example, \$SRIP\$, \$SRPRT\$, and so on.</li> </ul> <p>For more information on keyword functionality, see the topic, <i>"SIP Message Screening" in the ISC Application User Guide</i>.</p> |
| <b>Reg Ex Source Buffer</b> | <p>This parameter is used by the <b>Action Regular Expression</b> to apply the regular expression specified. If this parameter is not specified then it uses the content of the current BR.</p> <p>This parameter can contain one of the following values:</p> <ul style="list-style-type: none"> <li>• H1-H5, B1-B10, R1-R10, P1-P25</li> <li>• \c1-\c9</li> <li>• Keyword reference, for example, \$SRIP\$, \$SRPRT\$, and so on</li> </ul> <p>For more information on keyword functionality, see the topic, <i>"SIP Message Screening" in the ISC Application User Guide</i>.</p>   |
| <b>Regular Expression</b>   | <p>This parameter specifies a regular expression that applies to the content of the body attachment or to the content of the <b>Reg Ex Source Buffer</b> parameter.</p> <p>The action is only performed if the regular expression returns a match. The results of RegEx can be saved by using references \a1 - \a9 in the <b>Update String</b> parameter. This is useful to save only the parts of a body needed.</p>  |

| Parameter            | Description   |
|----------------------|---|
| <b>Response Code</b> | Enter a string of maximum of 3 characters length in the format NNN, where the corresponding ranges are (1 -6)(0 - 9)(0 - 9).<br><br>This parameter must be provisioned when the Body Rule <b>Action</b> parameter is set to <i>Reject</i> . |
| <b>Reason Phrase</b> | Enter a text string with a maximum length of 64 characters.<br><br>This is an optional parameter that specifies the reason phrase to be included with the response code.  |

- 5 Click OK.

**Result:** The SIP Filter Body Rule is added or modified.

For more information on the parameters see the topic “SIP Filter Body Rule” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision an SIP Filter Reference Rule

## Purpose

This procedure is used to provision an SIP Filter Reference Rule.

## Description

The purpose of creating an SIP Filter Reference Rule is to define the reference rules. For more information, see the topic, "*SIP Message Screening*" in the *ISC Application User Guide*.

## Before you begin

### Points to remember:

- Ensure that the SIP Filters are provisioned and disabled.
- Each SIP Filter can support only ten SIP Filter Reference Rules.

## Steps to provision an SIP Filter Reference Rule table

Perform the following steps at the Provisioning GUI:

---

1 Select **IMS → SIP Tables**.

**Result:** The **SIP Tables** window is displayed.

In the left pane, expand the **SIP Filter Reference Rule** folder.

**Result:** The SIP Filter Reference Rule tables are listed under the folder in the left pane.

If the folder is empty, add an SIP Filter Reference Rule table.

- 2** Perform the following steps in the **SIP Tables** window to add, rename, or delete an SIP Filter Reference Rule table:

| If you want to...                                      | Then...  |
|--|--|
| add an SIP Filter Reference Rule table,                | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add SIP Filter Reference Rule table</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |
| modify (or rename) an SIP Filter Reference Rule table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename SIP Filter Reference Rule table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p>   |
| delete an SIP Filter Reference Rule table,             | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p>   |

- 3** Double-click the desired SIP Filter Reference Rule table. The SIP Filter Reference Rule table opens in the right pane. Perform the following steps to add, modify, or delete the SIP Filter Reference Rule table attributes:

| If you want to ...                              | Then ...   |
|---|--|
| add SIP Filter Reference Rule table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Reference Rule</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol> |

| If you want to ...                                 | Then ...  |
|--|---|
| modify SIP Filter Reference Rule table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Reference Rule</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>              |
| delete SIP Filter Reference Rule table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> |

#### 4 Provision the following parameters:

**Note:**

- While provisioning the SIP Filter Reference Rule, the associated SIP Filter must be disabled.
- The **Conditions Fields** are used to specify the criteria that needs to be met to execute the action.
- The **Actions Fields** can be executed only if the result of the conditions are *true*.
- Depending on the action, only certain parameters are provisioned.

| Parameter                | Description   |
|--------------------------|---|
| <b>Filter ID</b>         | Select the filter ID that you want to associate with this Reference rule.   |
| <b>Reference Rule ID</b> | Select a unique Rule ID for the RR. The available values are 1 to 10.<br><b>Note:</b> Each SIP Filter can support only ten RRs.   |
| <b>Description</b>       | Enter the description of the Reference rule.  |
| <b>Case Sensitive</b>    | Specify if this rule applies to case sensitive ( <b>Yes</b> ) or case insensitive ( <b>No</b> ) character processing for content information.   |
| <b>Condition Fields</b>  |   |
| <b>Reference Name</b>    | <p>Enter the reference name that needs to be identified as a reference rule (RR).</p> <p>Reference rules are used as a "working rule" to reference previously saved data in the HR, BR, PR or RR and they perform validity checks or modify content. The content can be saved in an RR reference (for example, R1) without modifying the specified reference.</p> |

| Parameter                 | Description   |
|---------------------------|---|
| <b>Regular Expression</b> | <p>Enter the regular expression to evaluate the contents of the identified body attachment(s).</p> <p><b>Note:</b> RegExp allows more than nine references in a RegExp condition. However, only the first nine references can be referenced using \c1-c9 by other RR parameters.</p>  |
| <b>Boolean Condition</b>  | <p>Enter a logical Boolean expression using the RR base condition and the results of previous rule conditions.</p> <p>The RR base condition is defined by the previous condition fields in the present RR.</p> <p>The basic boolean operator symbols, “&amp;” (and), “ ”(or), “!” (not), parenthesis (to specify preference) are supported.</p> <p>A few examples (in R4):</p> <ul style="list-style-type: none"> <li>• R4 &amp; (! (H2   H3)) - This means that the condition is met if the base RR condition (R4) is true and neither of the conditions H2 or H3 are true.</li> <li>• !R4 applies negation to the RR base condition.</li> </ul>   |
| <b>Compare</b>            | <p>This parameter provides the ability to compare strings for example, string1 and string2.</p> <p>The following list gives the possible values for the argument passed in to the Compare Reference:</p> <ul style="list-style-type: none"> <li>• Reference to a previously saved Rule in that Filter (H1-5, B1-10, R1-10, or P1-25)</li> <li>• Backref from the Conditional Fields Regular Expression from that Rule (\c1-9)</li> <li>• Keyword value (\$\$SRIP\$, \$\$SRPRT\$, and so on)<br/>For more information on the keyword function, see the topic, "SIP Message Screening" in the ISC Application User Guide</li> <li>• Fixed string</li> </ul> <p>String1 and string2 can be compared based on:</p> <ul style="list-style-type: none"> <li>• Equal (for example, S1 = S2)</li> <li>• Subset (for example, S1 ⊆ S2)</li> <li>• Superset (for example, S2 ⊇ S1)</li> </ul> |
| <b>Occurrence</b>         | Select the number of times this rule is applied to the data before moving to the next rule.   |
| <b>Action Fields</b>      |   |

| Parameter            | Description  |
|----------------------|--|
| Action               | <p>Select an action type.</p> <p>The following are the available values:</p> <ul style="list-style-type: none"> <li>• <b>Modify</b> - To modify (or remove) the content of an identified reference.</li> <li>• <b>No Action</b> - Only conditional processing is done by the RR.</li> <li>• <b>Save</b> - To save the new content after applying this RR in memory for another rule to use in the same SIP Filter. Saved information is kept until all the rules in the SIP Filter have been processed. If no reference is specified then the RR is initialized with the value specified in the update string. The content can be empty.</li> </ul>  |
| Update String        | <p>Enter the value that will be used when the BR <b>Action</b> is set to <b>Modify</b>, <b>Save</b> and <b>Replace</b>. For <b>Modify</b> the content of the body is replaced with the content of this parameter. For <b>Save</b>, the content of the body or the content of this parameter is saved.</p> <p><b>Update String</b> values can be a combination of the following elements:</p> <ul style="list-style-type: none"> <li>• A text string enclosed by double quotes (for example, “abcd”).</li> <li>• Backrefs for referencing strings in the action field <b>RegularExpression</b> parameter. Valid format for backrefs is \a1 – \a9.</li> <li>• Backrefs for referencing strings in the condition field <b>RegularExpression</b> parameter. Valid format for backrefs is \c1 – \c9.</li> <li>• References to information saved by previous rule action (H1-H5, P1-P25, B1-B10, R1-R10).</li> <li>• A keyword value, for example, \$SRIPS\$, \$SRPRT\$, and so on. For more information on the keyword function, see the topic, "SIP Message Screening" in the ISC Application User Guide.</li> </ul> |
| Reg Ex Source Buffer | <p>This parameter is used by the <b>Regular Expression</b> to apply the regular expression specified. If this parameter is not specified then it uses the content of the current RR.</p> <p>This parameter can contain one of the following values:</p> <ul style="list-style-type: none"> <li>• H1-H5, B1-B10, R1-R10, P1-P25</li> <li>• \c1-\c9</li> <li>• Keyword reference, for example, \$SRIPS\$, \$SRPRT\$</li> </ul> <p>For more information on keyword functionality, see the topic, "SIP Message Screening" in the ISC Application User Guide.</p>   |

| Parameter                 | Description  |
|---------------------------|--|
| <b>Regular Expression</b> | This parameter specifies a regular expression that applies to the content of the body attachment or to the content of the “RegEx Source Buffer” parameter.<br><br>The action is only performed if the regular expression returns a match. The results of RegEx can be saved by using references \a1 - \a9 in the <b>Update String</b> parameter. This is useful to save only the parts of a body needed. |

- 5 Click **OK**.

**Result:** The SIP Filter Reference Rule is added or modified.

For more information on the parameters, see the topic “SIP Filter Reference Rule” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision an SIP Filter Parameter Rule

## Purpose

This procedure is used to provision an SIP Filter Parameter Rule.

## Description

The purpose of creating an SIP Filter Parameter Rule is to define the parameter rules. For more information, see the topic, "*SIP Message Screening*" in the *ISC Application User Guide*.

## Before you begin

### Points to remember:

- Ensure that the SIP Filters are provisioned and disabled.
- Ensure that the SIP Filter Header Rules are provisioned.
- Each SIP Filter Header Rule can support five SIP Parameter Rules.
- Each SIP Filter can support five HRs and twenty-five PRs (that is, five PRs per HR).

## Steps to provision an SIP Filter Parameter Rule table

Perform the following steps at the Provisioning GUI:

- 
- 1 Navigate to **IMS → SIP Tables**.

**Result:** The **SIP Tables** window is displayed.

In the left pane, expand the **SIP Filter Parameter Rule** folder.

**Result:** The SIP Filter Parameter Rule tables are listed under the folder in the left pane.

If the folder is empty, add an SIP Filter Parameter Rule table.

- 2** Perform the following steps in the **SIP Tables** window to add, rename, or delete an SIP Filter Parameter Rule table:

| If you want to...                                      | Then...  |
|--|--|
| add an SIP Filter Parameter Rule table,                | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add SIP Filter Parameter Rule table</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |
| modify (or rename) an SIP Filter Parameter Rule table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Add SIP Filter Parameter Rule table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p>  |
| delete an SIP Filter Parameter Rule table,             | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p>   |

- 3** Double-click the desired SIP Filter Parameter Rule table. The SIP Filter Parameter Rule table opens in the right pane. Perform the following steps to add, modify, or delete the SIP Filter Parameter Rule table attributes:

| If you want to ...                              | Then ...  |
|---|---|
| add SIP Filter Parameter Rule table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Filter Parameter Rule</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol> |

| If you want to ...                                 | Then ...  |
|--|---|
| modify SIP Filter Parameter Rule table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Filter Parameter Rule</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>   |
| delete SIP Filter Parameter Rule table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> |

#### 4 Provision the following parameters:

**Note:**

- While provisioning the SIP Parameter Rule, the associated SIP Filter must be disabled.
- The **Conditions Fields** are used to specify the criteria that needs to be met to execute the action.
- The **Actions Fields** can be executed only if the result of the conditions are *true*.
- Depending on the action, only certain parameters are provisioned.

| Parameter           | Description   |
|---------------------|---|
| <b>Filter ID</b>    | Select the filter ID that you want to associate with this PR.   |
| <b>Header ID</b>    | Select the header ID that you want to associate with this PR.   |
| <b>Parameter ID</b> | Select a unique parameter ID for the PR. The available values are 1 to 25.<br><b>Note:</b> Each SIP Filter can support only twenty-five PRs (that is, five PRs per HR). |
| <b>Description</b>  | Enter the description of the parameter rule.  |

| Parameter                 | Description   |
|---------------------------|---|
| <b>Case Sensitive</b>     | <p>The two options available are:</p> <ul style="list-style-type: none"> <li>• Choose <b>Yes</b> to select case sensitive.</li> <li>• Choose <b>No</b> to select case insensitive.</li> <li>• The default value is <b>No</b>.</li> </ul> <p>This parameter specifies if this rule applies case sensitive or case insensitive character processing for the content of the identified header. This parameter applies to the condition and action of this rule.</p>  |
| <b>Condition Fields</b>   |   |
| <b>Parameter Type</b>     | Select the parameter type in the header. The available values are <b>None</b> , <b>User</b> , <b>URI</b> , or <b>Header</b> .   |
| <b>Parameter String</b>   | Enter the name of the parameter to be searched in the header. For example, CIC.   |
| <b>Regular Expression</b> | <p>Enter regular expressions to match and analyze the content of the parameter.</p> <p><b>Note:</b> The Regular Expression is used to select the information from the content of the parameter. For example, if the parameter has no value (null), then the regular expression returns false. The result of this regular expression changes the value result of the PR (true or false).</p> <p>RegExp allows more than nine references in a RegExp condition. However, only the first nine references can be referenced using \c1-c9 by other PR parameters.</p> <p>When grouping is used in the expression, the backrefs can be accessed in the rule. For example \c2. Where “c” identifies the back ref as a condition regex backref.</p> |

| Parameter                | Description  |
|--------------------------|--|
| <b>Boolean Condition</b> | <p>Enter a logical Boolean expression using the BR base condition and the results of previous rule conditions. The BR base condition is defined by the previous condition fields in the present BR. The HRs and PRs have Boolean values, that is either True or False values depending on the results of the execution.</p> <p>The stored value and rule value (HR or PR) exist only with in the scope of the Filter. This information is released when the filter is executed.</p> <p>The parameter supports basic boolean operator symbols, “&amp;” (and), “ ” (or), “!” (not), and parentheses (to specify preference).</p> <p>A few examples (in B4):</p> <ul style="list-style-type: none"> <li>• B4 &amp; (! (H2   H3)) - This means that the condition is met if the base BR condition (B4) is true and neither of the conditions H2 or H3 are true.</li> <li>• !B4 applies negation to the BR base condition.</li> </ul> <p><b>Note:</b> The HR and PRs can be referenced by “H” and ID number, and “P” and ID number respectively. Spaces are not allowed in a Boolean condition.</p> |
| <b>Compare</b>           | <p>This parameter provides the ability to compare strings for example, string1 and string2.</p> <p>The following list gives the possible values for the argument passed in to the Compare Reference:</p> <ul style="list-style-type: none"> <li>• Reference to a previously saved Rule in that Filter (H1-H5, B1-B10, R1-R10, or P1-P25)</li> <li>• Backref from the Conditional Fields Regular Expression from that Rule (\c1-9)</li> <li>• Keyword reference, for example, \$SRIPS\$, \$SRPRT\$, and so on<br/>For more information on the keyword function, see the topic, "<i>SIP Message Screening</i>" in the <i>ISC Application User Guide</i>.</li> <li>• Fixed string</li> </ul> <p>Comparison of string1 and string2 can be for the following conditions:</p> <ul style="list-style-type: none"> <li>• Equal (for example, S1 = S2)</li> <li>• Subset (for example, S1 ⊆ S2)</li> <li>• Superset (for example, S2 ⊇ S1)</li> </ul>   |
| <b>Action Fields</b>     |  |

| Parameter          | Description   |
|--------------------|---|
| Action             | <p>Select an action to be taken when the conditions are met.</p> <ul style="list-style-type: none"> <li>• <b>No action</b> - Evaluates the PR.</li> <li>• <b>Add</b> - Adds a new parameter (type must be specified). The new parameter can contain a value (Update String is optional). For example, cic=281 or LC.</li> <li>• <b>Remove</b> - Deletes the parameter specified in the Condition parameter.</li> <li>• <b>Modify</b> - Modifies the content of the Parameter using Update String values or removes the content of the Parameter.</li> <li>• <b>Save</b> - Saves the content of the Parameter or Update String.</li> </ul>   |
| New Parameter type | <p>Select the type of parameter that needs to be added. The available values are: <b>Header</b>, <b>None</b>, <b>URI</b>, and <b>User</b>.</p> <p><b>Note:</b> Parameters cannot be manipulated with user-defined headers. For example, ‘X-MYHEADER: ’.</p>   |
| New Parameter name | Enter the name of the new parameter that needs to be added.   |
| Update String      | <p><b>Update String</b> values can be a combination of the following elements:</p> <ul style="list-style-type: none"> <li>• A text string enclosed by double quotes (for example, “abcd”).</li> <li>• Backrefs for referencing strings in the action field <b>RegularExpression</b> parameter. Valid format for backrefs is \a1 – \a9.</li> <li>• Backrefs for referencing strings in the condition field <b>RegularExpression</b> parameter. Valid format for backrefs is \c1 – \c9.</li> <li>• References to information saved by previous rule action (H1-H5, P1-P25, B1-B10, R1-R10).</li> <li>• A keyword value, for example, \$SRIP\$, \$SRPRT\$, and so on.</li> </ul> <p>For more information in the keyword function, see the topic, <i>“SIP Message Screening” in the ISC Application User Guide</i>.</p> |

| Parameter                   | Description  |
|-----------------------------|--|
| <b>Reg Ex Source Buffer</b> | <p>Enter the text string.</p> <p>The action <b>Regular Expression</b> uses this parameter to apply the regular expression specified. If not specified, it uses the content of the current PR.</p> <p>This parameter can contain one of the following:</p> <ul style="list-style-type: none"> <li>• H1-H5, B1-B10, R1-R10, P1-P25</li> <li>• \c1-\c9</li> <li>• Keyword reference, for example, \$SRIP\$, \$SRPRT\$ and so on</li> </ul> <p>For more information on the keyword function, see the topic, "<i>SIP Message Screening</i>" in the <i>ISC Application User Guide</i>.</p>   |
| <b>Regular Expression</b>   | <p>Enter regular expressions to analyze the content of the parameter.</p> <p>The result of this parameter that is, backref format is used conditionally to add a new parameter, update existing parameter or save specific information from the parameter content.</p> <p>If specific content needs to be saved, then the Update String and the Regular Expression can be used simultaneously. The save operation is executed only if the return of the RegEx is a match.</p> <p>For example, to save only the IP address content (IPV4) of the header, enter Regular Expression =([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}):[0-9]{1,4}) and the backref in the Update String =\a1.</p> <p>The action backref syntax changes from \1-9 to \a1-9.</p> |

5 Click OK.

**Result:** The SIP Filter Parameter Rule is added or modified.

For more information on the parameters, see the topic "SIP Filter Parameter Rule" in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision an SIP Filter Set

## Purpose

This procedure is used to provision an SIP Filter Set.

## Description

The purpose of creating an SIP Filter Set is to assign one or more SIP Filters to an SIP Filter Set. For more information, see the topic, "*SIP Message Screening*" in the *ISC Application User Guide*.

## Before you begin

### Points to remember:

- Ensure that the SIP Filters and optionally, SIP Filter Header Rules and SIP Parameter Rules are provisioned.
- Each Filter Set can support a maximum of 600 SIP Filters.
- Ensure that the existing SIP Filter set is not assigned to a component (PCSCF or IBCF).

## Steps to provision an SIP Filter Set

Perform the following steps at the Provisioning GUI:

---

1 Select **IMS → SIP Tables**.

**Result:** The **SIP Tables** window is displayed.

In the left pane, expand the **SIP Filter Set** folder.

**Result:** The SIP Filter Set tables are listed under the folder in the left pane.

If the folder is empty, add an SIP Filter Set table.

- 2 Perform the following steps in the **SIP Tables** window to add, rename, or delete an SIP Filter Set table:

| If you want to...                           | Then...   |
|---|---|
| add an SIP Filter Set table,                | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add SIP Filter Set table</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |
| modify (or rename) an SIP Filter Set table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename SIP Filter Set table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p>   |
| delete an SIP Filter Set table,             | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p>  |

- 3 Double-click the desired SIP Filter Set table. The SIP Filter Set table opens in the right pane. Perform the following steps to add, modify, or delete the SIP Filter Set table attributes:

| If you want to ...                   | Then ...   |
|--------------------------------------|--|
| add SIP Filter Set table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Filter Set</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol> |

| If you want to ...                      | Then ...  |
|---|---|
| modify SIP Filter Set table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Filter Set</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>              |
| delete SIP Filter Set table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> |

**4** Provision the following parameters:

| Parameter          | Description   |
|--------------------|---|
| <b>Filter Set</b>  | Enter a unique filter set Id.   |
| <b>Description</b> | Enter a description for the filter set.   |
| <b>SIP Filter</b>  | <p>The available SIP filters are displayed in the <b>Available Filters</b> parameters.</p> <p>Use the <b>Add</b> and <b>Delete</b> to select and set the order of the filters in the <b>Filters in the Set</b> parameters.</p> <p><b>Note:</b> Each Filter Set can support a maximum of 20 SIP Filters.</p> |

**5** Click **OK**.

**Result:** The SIP Filter Set is added or modified.

For more information on the parameters, see the topic “SIP Filter Set” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision priority mode

## Overview

### Purpose

This section provides the procedure to provision the Priority Mode.

### Contents

|  |      |
|--|------|
| <a href="#">To provision an Emergency Identifiers List</a> | 5-61 |
| <a href="#">To provision an NGN GETS Identifier List</a>   | 5-64 |

# To provision an Emergency Identifiers List

## Purpose

This procedure is used to provision an Emergency Identifiers List.

## Description

The purpose of creating an Emergency Identifiers List is to define the emergency identifier digit string.

## Steps to provision an Emergency Identifiers List table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS** → **IMS Tables** → **IMS** → **General**. Expand the **Emergency Identifiers List** folder if the folder is not empty.

**Result:** The Emergency Identifiers List table is listed under the folder in the left pane.  
If the folder is empty, add an Emergency Identifiers List table.

---

- 2 Perform the following steps in the **IMS Tables** window to add, rename, or delete an Emergency Identifiers List table:

| If you want to...                        | Then...  |
|--|--|
| add an Emergency Identifiers List table, | <ol style="list-style-type: none"><li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add Emergency Identifiers List table</b> window is displayed.</li><li>From the <b>Table Number</b> list, select the table number.</li><li>In the <b>Table Name</b> box, type a descriptive table name.</li><li>Click <b>OK</b>.</li></ol> <p><i>End of steps.</i></p> |

| If you want to...                           | Then...   |
|---|---|
| rename an Emergency Identifiers List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename Emergency Identifiers List table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |
| delete an Emergency Identifiers List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p>  |

- 3 Double-click the Emergency Identifiers List table. The Emergency Identifiers List table opens in the right pane. Perform the following steps to add, modify, or delete the Emergency Identifiers List table attributes:

| If you want to ...                                  | Then ...   |
|---|--|
| add Emergency Identifiers List table attributes,    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Emergency Identifiers</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>  |
| modify Emergency Identifiers List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Emergency Identifiers</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>       |
| delete Emergency Identifiers List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> |

- 
- 4 Provision the following parameters:

| Parameter             | Description   |
|-----------------------|---|
| ID                    | Select a unique ID for the Emergency Identifier from the list.  |
| Emergency Identifiers | Enter a digit string in the <b>Emergency Identifiers</b> field. |

---

- 5 Click **OK**.

**Result:** The Emergency Identifiers List attribute is added or modified.

For more information about the parameters, refer to the topic “Emergency Identifiers List” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

---

# To provision an NGN GETS Identifier List

## Purpose

This procedure is used to provision an NGN GETS Identifier List.

## Description

The purpose of creating an NGN GETS Identifier List is to define the AN/NT identifier digit string.

## Before you begin

### Points to remember:

- Only one table is allowed under the NGN GETS Identifier List.
- A maximum of 15 AN/NT identifiers can be provisioned in the NGN GETS Identifier List table.

## Steps to provision an NGN GETS Identifier List List table

Perform the following steps at the Provisioning GUI:

- 
- 1** Select **IMS → Global Tables**. Expand the **NGN GETS Identifier List** folder if the folder is not empty.

In the left pane, expand the **NGN GETS Identifier List** folder.

**Result:** The NGN GETS Identifier List table is listed under the folder in the left pane.  
If the folder is empty, add an NGN GETS Identifier List table.

- 
- 2** Perform the following steps in the **Global Tables** window to add, rename, or delete an NGN GETS Identifier List table:

| If you want to...                      | Then...  |
|--|--|
| add an NGN GETS Identifier List table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add NGN GETS Identifier List table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |

| If you want to...                         | Then...   |
|---|---|
| rename an NGN GETS Identifier List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename NGN GETS Identifier List table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |
| delete an NGN GETS Identifier List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p>  |

- 3 Double-click the NGN GETS Identifier List table. The NGN GETS Identifier List table opens in the right pane. Perform the following steps to add, modify, or delete the NGN GETS Identifier List table attributes:

| If you want to ...                                | Then ...   |
|---|--|
| add NGN GETS Identifier List table attributes,    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>NGN GETS Identifier</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>  |
| modify NGN GETS Identifier List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>NGN GETS Identifier</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>         |
| delete NGN GETS Identifier List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> |

---

**4** Provision the following parameters:

| Parameter           | Description  |
|---------------------|--|
| AN/NT Identifier ID | Select an unique ID for the AN/NT Identifier. The available values are 1-15.   |
| AN/NT Identifier    | Enter a string of three to ten digits. The available values are 0-9.<br><b>Note:</b> This string is used as a matching criteria, when processing an address contained within the R-URI in support of either a GETS-AN or GETS-NT invoked call. |

---

**5** Click **OK**.

**Result:** The NGN GETS Identifier List is added or modified.

For more information about the parameters, refer to the topic “NGN GETS Identifier List” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

---

# To provision security gateway

## Overview

### Purpose

This section provides the procedure to provision the Security Gateway.

### Contents

|   |      |
|---|------|
| To provision an SIP Flow Trusted/Untrusted Rate Limit Rule Set      | 5-68 |
| To provision an SIP Aggregate Trusted/Untrusted Rate Limit Rule Set | 5-72 |
| To provision a Flow Source Address Policy                           | 5-76 |
| To provision an Aggregate Source Address Policy                     | 5-80 |
| To provision a Registration Failure Policy                          | 5-83 |
| To provision an Application Layer Policy                            | 5-87 |
| To provision a Security Gateway Profile                             | 5-90 |

# To provision an SIP Flow Trusted/Untrusted Rate Limit Rule Set

## Purpose

This procedure is common for both SIP Flow Trusted Rate Limit Rule Set and SIP Flow Untrusted Rate Limit Rule Set. Follow the steps to add, modify or delete an SIP Flow Trusted Rate Limit Rule Set, or an SIP Flow Untrusted Rate Limit Rule Set.

### Procedure to add, rename, or delete the SIP Flow Trusted/Untrusted Rate Limit Rule Set table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → SIP Tables**.
- 2 Expand the **SIP Flow Trusted Rate Limit Rule Set** folder, or click the **SIP Flow Trusted Rate Limit Rule Set** folder, if the folder is still empty.

**Note:** For SIP Flow Untrusted Rate Limit Rule Set, replace **SIP Flow Trusted Rate Limit Rule Set** in the above step with **SIP Flow Untrusted Rate Limit Rule Set** .

3

| If you want to...   | then...  |
|---|--|
| add a table in the <b>SIP Flow Trusted Rate Limit Rule Set</b> folder,      | <ol style="list-style-type: none"> <li>1. Right-click <b>SIP Flow Trusted Rate Limit Rule Set</b> and select <b>Add Table</b>.<br/><b>Note:</b> For SIP Flow Untrusted Rate Limit Rule Set, replace <b>SIP Flow Trusted Rate Limit Rule Set</b> in the above step with <b>SIP Flow Untrusted Rate Limit Rule Set</b> .</li> <li>2. Select a unique number from the <b>Table Number</b> list.</li> <li>3. Enter a unique name in the <b>Table Name</b> field.</li> <li>4. Click <b>OK</b>.<br/><i>End of steps</i></li> </ol> |
| rename the table in the <b>SIP Flow Trusted Rate Limit Rule Set</b> folder, | <ol style="list-style-type: none"> <li>1. Right-click the desired table and select <b>Rename Table</b>.</li> <li>2. Enter the required table name and click <b>OK</b>.<br/><i>End of steps</i></li> </ol>  |

| If you want to...   | then...  |
|---|--|
| delete the table in the <b>SIP Flow Trusted Rate Limit Rule Set</b> folder, | <ol style="list-style-type: none"> <li>Right-click the desired table and select <b>Delete Table</b>.</li> <li>Click <b>Yes</b> to confirm the deletion.</li> </ol> <i>End of steps</i> |

**Notes:**

- For SIP Flow Untrusted Rate Limit Rule Set, replace **SIP Flow Trusted Rate Limit Rule Set** in the above table with **SIP Flow Untrusted Rate Limit Rule Set**.

END OF STEPS

### Procedure to provision the table attributes

Perform the following steps at the Provisioning GUI:

1 Navigate to **IMS > SIP Tables**.

2 Expand the **SIP Flow Trusted Rate Limit Rule Set** folder, or click the **SIP Flow Trusted Rate Limit Rule Set** folder, if the folder is still empty.

**Note:** For SIP Flow Untrusted Rate Limit Rule Set, replace **SIP Flow Trusted Rate Limit Rule Set** in the above step with **SIP Flow Untrusted Rate Limit Rule Set**.

**Note:** For SIP Flow Untrusted Rate Limit Rule Set, replace **SIP Flow Trusted Rate Limit Rule Set** in the above step with **SIP Flow Untrusted Rate Limit Rule Set**.

3 Right-click the table and select **Open**.

4 Click **Attributes**.

| 5 If you want to...      | then...   |
|--------------------------|---|
| add table attributes,    | select <b>Add Table Attributes</b> and proceed with <a href="#">Step 6</a> .    |
| modify table attributes, | select <b>Modify Table Attributes</b> and proceed with <a href="#">Step 6</a> . |

| If you want to...        | then...  |
|--------------------------|--|
| delete table attributes, | <p>Perform the following steps.</p> <ol style="list-style-type: none"> <li>1. Right-click the desired profile and select <b>Delete Table Attributes</b>.</li> <li>2. Click <b>Yes</b> to confirm.<br/><i>End of steps</i></li> </ol> |

6 Select a unique number in the **Rule Id** list.

7 Enter a brief description in the **Description** field.

8 Select the SIP message/response that requires screening from the **SIP Message Type** box and click **Add**, to add it to the **SIP Message List**.

If required, multiple SIP messages/responses can be added to group them under the set **Rule Id**.

**Note:** To remove a selected SIP message/response from the **SIP Message List**, use the **Delete** button .

9 Review the **Rate Limit** and the **Source Granularity** for the selected SIP messages/responses.

The values in these fields is applicable to all the SIP messages/responses in the **SIP Message List**.

The available options for the **Rate Limit** are:

- drop all
- no limit
- <enter 1 - 10000>
- 1

**Note:** Alcatel-Lucent recommends retaining the default values.

10 Click **OK**.

**Result:** A new SIP Flow Trusted (or Untrusted) Rate Limit rule set is added.

For more information on the parameters see the topic “IMS - SIP Tables” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision an SIP Aggregate Trusted/Untrusted Rate Limit Rule Set

## Purpose

The procedure described in this topic is common for both SIP Aggregate Trusted Rate Limit Rule Set and SIP Aggregate Untrusted Rate Limit Rule Set. This procedure is used to provision an SIP Aggregate Trusted Rate Limit Rule Set, or a SIP Aggregate Untrusted Rate Limit Rule Set.

## Steps to provision an SIP Aggregate Trusted/Untrusted Rate Limit Rule Set table

Perform the following steps at the Provisioning GUI:

---

### 1 Select IMS → SIP Tables.

**Result:** The **SIP Tables** window is displayed.

In the left pane, expand the **SIP Aggregate Trusted Rate Limit Rule Set** folder.

**Result:** The SIP Aggregate Trusted Rate Limit Rule Set tables are listed under the folder in the left pane.

If the folder is empty, add an SIP Aggregate Trusted Rate Limit Rule Set table.

**Note:** For SIP Aggregate Untrusted Rate Limit Rule Set, replace **SIP Aggregate Trusted Rate Limit Rule Set** in the above step with **SIP Aggregate Untrusted Rate Limit Rule Set**.

---

### 2 Perform the following steps in the **SIP Tables** window to add, rename, or delete an SIP Aggregate Trusted Rate Limit Rule Set table:

| If you want to...  | then...   |
|--|---|
| add an <b>SIP Aggregate Trusted Rate Limit Rule Set</b> table, | <ol style="list-style-type: none"> <li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add SIP Aggregate Trusted Rate Limit Rule Set table</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |

| If you want to...   | then...  |
|---|--|
| rename an <b>SIP Aggregate Trusted Rate Limit Rule Set</b> table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename SIP Aggregate Trusted Rate Limit Rule Set table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |
| delete an <b>SIP Aggregate Trusted Rate Limit Rule Set</b> table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p>   |

**Notes:**

- For SIP Aggregate Untrusted Rate Limit Rule Set, replace **SIP Aggregate Trusted Rate Limit Rule Set** in the above table with **SIP Aggregate Untrusted Rate Limit Rule Set**.
- There are default values for rate limits in a newly created rule set.

- 3 Double-click the desired SIP Aggregate Trusted Rate Limit Rule Set table. The SIP Aggregate Trusted Rate Limit Rule Set table opens in the right pane. Perform the following steps to add, modify, or delete the SIP Aggregate Trusted Rate Limit Rule Set table attributes:

| If you want to ...   | Then ...   |
|--|--|
| add SIP Aggregate Trusted Rate Limit Rule Set table attributes,    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Aggregate Trusted Rate Limit Rule</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>  |
| modify SIP Aggregate Trusted Rate Limit Rule Set table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Aggregate Trusted Rate Limit Rule</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol> |

| If you want to ...   | Then ...   |
|--|--|
| delete SIP Aggregate Trusted Rate Limit Rule Set table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> |

**Note:** For SIP Aggregate Untrusted Rate Limit Rule Set, replace **SIP Aggregate Trusted Rate Limit Rule Set** in the above table with **SIP Aggregate Untrusted Rate Limit Rule Set**

**4** Provision the following parameters:

| Parameter               | Description   |
|-------------------------|---|
| <b>Rule Id</b>          | Select a unique number in the <b>Rule Id</b> list.  |
| <b>Description</b>      | Enter a brief description in the <b>Description</b> field.  |
| <b>SIP Message List</b> | <p>Select the SIP message or response that requires screening from the <b>SIP Message List</b> box and click <b>Add</b>, to add it to the <b>Selected SIP Message</b> box.</p> <p>If required, multiple SIP messages or responses can be added to group them under the set <b>Rule Id</b>.</p> <p><b>Note:</b> To remove a selected SIP message or response from the <b>Selected SIP Message</b> box, use the <b>Delete</b> button .</p>                                  |
| <b>Rate Limit</b>       | <p>Select the <b>Rate Limit</b> for the selected SIP messages or responses.</p> <p>The values in this field are applicable to all the SIP messages or responses in the <b>SIP Message List</b> box.</p> <p>The available options are:</p> <ul style="list-style-type: none"> <li>• drop all</li> <li>• no limit</li> <li>• &lt;enter 1 - 20000&gt;</li> <li>• 1000 (Default value)</li> </ul> <p><b>Note:</b> Alcatel-Lucent recommends retaining the default values.</p> |

**5** Click **OK**.

**Result:** A new SIP Aggregate Trusted (or Untrusted) Rate Limit rule set is added.

For more information on the parameters, see the topic “SIP Aggregate Trusted (or Untrusted) Rate Limit Rule Set” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision a Flow Source Address Policy

## Purpose

This procedure provides the steps to provision a Flow Source Address Policy.

## Steps to provision a Flow Source Address Policy table

Perform the following steps at the Provisioning GUI:

**1** Select **IMS → SIP Tables**.

**Result:** The **SIP Tables** window is displayed.

In the left pane, expand the **Flow Source Address Policy** folder.

**Result:** The Flow Source Address Policy table is listed under the folder in the left pane.

If the folder is empty, add a Flow Source Address Policy table.

**2** Perform the following steps in the **SIP Tables** window to add, rename, or delete a **Flow Source Address Policy** table:

| If you want to...                                   | then...  |
|---|--|
| add a <b>Flow Source Address Policy</b> table       | <ol style="list-style-type: none"> <li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add Flow Source Address Policy</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |
| rename the <b>Flow Source Address Policy</b> table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Rename Flow Source Address Policy</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p>   |

| If you want to...                                   | then...  |
|---|--|
| delete <b>Flow Source Address Policy</b> the table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p> |

- 3 Double-click the Flow Source Address Policy table. The Flow Source Address Policy table opens in the right pane. Perform the following steps to add, modify, or delete the Flow Source Address Policy table attributes:

| If you want to ...                                  | Then ...   |
|---|--|
| add Flow Source Address Policy table attributes,    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Source Address Policy</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>  |
| modify Flow Source Address Policy table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Source Address Policy</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>       |
| delete Flow Source Address Policy table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> |

- 4 Provision the following parameters:

| Parameter          | Description   |
|--------------------|---|
| <b>Policy Id</b>   | Select a unique number from the <b>Policy Id</b> list.                      |
| <b>Description</b> | Enter a brief description in the <b>Description</b> field.                  |
| <b>Policy Type</b> | Select the <b>Policy Type</b> that you would like to assign to this policy. |

| Parameter                              | Description  |
|--|--|
| <b>SIP Flow Rate Limit Rule Set Id</b> | Select the Rule Id of the SIP Flow Rate Limit Rule Set (Trusted/Untrusted), that you intend to associate with this policy, in the <b>SIP Flow Rate Limit Rule Set Id</b> list.   |
| <b>Compressed Message Rate Limit</b>   | <p>Select a value from the <b>Compressed Message Rate Limit</b> list.</p> <p>This parameter specifies the number of Sigcomp compressed SIP message that are allowed to be received per minute from trusted or untrusted IP source. The available options are:</p> <ul style="list-style-type: none"> <li>• drop all</li> <li>• no limit</li> <li>• &lt;enter 1 - 20000&gt;</li> <li>• 1000</li> </ul> <p><b>Note:</b> Alcatel-Lucent recommends retaining the default value.</p> |
| <b>Keep-Alive Message Rate Limit</b>   | <p>Select a value from the <b>Keep-Alive Message Rate Limit</b> list.</p> <p>This field specifies the number of Keep-Alive messages that are allowed to be received per minute from a trusted/untrusted IP address. It applies to all the UDP (STUN) and TCP (CRLF) traffic. Here,</p> <ul style="list-style-type: none"> <li>• drop all</li> <li>• no limit</li> <li>• &lt;enter 1 - 10000&gt;</li> <li>• 1</li> </ul>  |
| <b>Maximum Message Size</b>            | <p>Enter the maximum size of the SIP message to be allowed through in the <b>Maximum Message Size</b> field.</p> <p>In this field, “0” indicates no limit imposed.</p>   |
| <b>Attack Quarantine Time</b>          | <p>Enter the time frame in the <b>Attack Quarantine Time</b> field.</p> <p>This field indicates the time frame in minutes, during which a source IP address and port number will be placed in quarantine, when any of the Security Gateway policies/rates are exceeded.</p> <p>In this field, “0” indicates no quarantine imposed.</p>   |

5 Click OK.

**Result:** A new Flow Source Address policy is added.

For more information on the parameters, see the topic “Flow Source Address policy” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision an Aggregate Source Address Policy

## Purpose

This procedure describes the steps to provision an Aggregate Source Address Policy.

## Steps to provision an Aggregate Source Address Policy table

Perform the following steps at the Provisioning GUI:

**1** Select **IMS → SIP Tables**.

**Result:** The **SIP Tables** window is displayed.

In the left pane, expand the **Aggregate Source Address Policy** folder.

**Result:** The Aggregate Source Address Policy table is listed under the folder in the left pane.

If the folder is empty, add an Aggregate Source Address Policy table.

**2** Perform the following steps in the **SIP Tables** window to add, rename, or delete an Aggregate Source Address Policy table:

| If you want to...  | then...   |
|--|---|
| add an Aggregate Source Address Policy table,                | <ol style="list-style-type: none"> <li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add Aggregate Source Address Policy table</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |
| modify (or rename) an Aggregate Source Address Policy table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Rename Aggregate Source Address Policy table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p>   |

| If you want to...                                     | then...  |
|---|--|
| delete an Aggregate Source Address Policy Rule table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p> |

- 3 Double-click the Aggregate Source Address Policy table. The Aggregate Source Address Policy table opens in the right pane. Perform the following steps to add, modify, or delete the Aggregate Source Address Policy table attributes:

| If you want to ...                                       | Then ...   |
|--|--|
| add Aggregate Source Address Policy table attributes,    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Aggregate Policy</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>   |
| modify Aggregate Source Address Policy table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Aggregate Policy</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>            |
| delete Aggregate Source Address Policy table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> |

- 4 Provision the following parameters:

| Parameter          | Description   |
|--------------------|---|
| <b>Policy Id</b>   | Select a unique number from the <b>Policy Id</b> list.                      |
| <b>Description</b> | Enter a brief description in the <b>Description</b> field.                  |
| <b>Policy Type</b> | Select the <b>Policy Type</b> that you would like to assign to this policy. |

| Parameter                                   | Description  |
|---|--|
| <b>SIP Aggregate Rate Limit Rule Set Id</b> | <p>Select the Rule Id of the SIP Aggregate Rate Limit Rule Set (Trusted/Untrusted), that you intend to associate with this policy, in the <b>SIP Aggregate Rate Limit Rule Set Id</b> list.</p>  |
| <b>Compressed Message Rate Limit</b>        | <p>Select a value from the <b>Compressed Message Rate Limit</b> list.</p> <p>This parameter specifies the number of Sigcomp compressed SIP message that are allowed to be received per minute from trusted or untrusted IP source. The available options are:</p> <ul style="list-style-type: none"> <li>• drop all</li> <li>• no limit</li> <li>• &lt;enter 1 - 20000&gt;</li> <li>• 1000</li> </ul> <p><b>Note:</b> Alcatel-Lucent recommends retaining the default value.</p> |
| <b>Keep-Alive Message Rate Limit</b>        | <p>Select a value from the <b>Keep-Alive Message Rate Limit</b> list.</p> <p>This parameter specifies the number of Keep-Alive messages that are allowed to be received per minute from a trusted/untrusted IP address. It applies to all the UDP (STUN) and TCP (CRLF) traffic. The available options are:</p> <ul style="list-style-type: none"> <li>• drop all</li> <li>• no limit</li> <li>• &lt;enter 1 - 20000&gt;</li> <li>• 1000</li> </ul>                              |

**5** Click **OK**.

**Result:** A new Aggregate Source Address Policy is added.

For more information on the parameters, see the topic “Aggregate Source Address Policy”om in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision a Registration Failure Policy

## Purpose

This procedure is used to provision a Registration Failure Policy.

## Steps to provision a Registration Failure Policy table

Perform the following steps at the Provisioning GUI:

**1** Select **IMS → SIP Tables**.

**Result:** The **SIP Tables** window is displayed.

In the left pane, expand the **Registration Failure Policy** folder.

**Result:** The Registration Failure Policy table is listed under the folder in the left pane.

If the folder is empty, add a Registration Failure Policy table.

**2** Perform the following steps in the **SIP Tables** window to add, rename, or delete a Registration Failure Policy table:

| If you want to...                                       | then...   |
|---|---|
| add a Registration Failure Policy table,                | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add Registration Failure Policy table</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <i>End of steps.</i> |
| modify (or rename) a Registration Failure Policy table, | <ol style="list-style-type: none"><li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Rename Registration Failure Policy table</b> window is displayed.</li><li>2. In the <b>Table Name</b> box, type a new table name.</li><li>3. Click <b>OK</b>.</li></ol> <i>End of steps.</i>   |

| If you want to...                                | then...  |
|--|--|
| delete a Registration Failure Policy Rule table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p> |

- 3** Double-click the Registration Failure Policy table. The Registration Failure Policy table opens in the right pane. Perform the following steps to add, modify, or delete the Registration Failure Policy table attributes:

| If you want to ...                                   | Then ...  |
|--|---|
| add Registration Failure Policy table attributes,    | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Aggregate Policy</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>  |
| modify Registration Failure Policy table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Registration Failure Policy</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol> |
| delete Registration Failure Policy table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> |

- 4** Provision the following parameters:

| Parameter          | Description   |
|--------------------|---|
| <b>Policy ID</b>   | Select the Registration Failure Policy ID from the <b>Policy ID</b> list.           |
| <b>Description</b> | In the <b>Description</b> field, enter the Registration Failure Policy Description. |

| Parameter                           | Description  |
|-------------------------------------|--|
| Registration Control Interval (sec) | In the <b>Registration Control Interval (sec)</b> field, enter the time in seconds, any value from 10 to 300. This field specifies the amount of time, in seconds, that a source IP address and port number are allowed to get a successful registration after having an initial REGISTER rejected with 403 “Forbidden” response by the S-CSCF. If no successful registration occurs, then the source is put into quarantine.  |
| Max Attempts                        | <p>In the <b>Max Attempts</b> field, select from the following available options:</p> <ul style="list-style-type: none"> <li>• A value that ranges from 2 to 10</li> <li>• 0</li> </ul> <p>This field specifies the number of times a REGISTER attempt and failure are allowed from the source for initial registration during the specified interval above.</p> <p>When the maximum number of REGISTER attempts reaches this configured value, and no success response returned from the S-CSCF (200 OK), then the source is put into quarantine.</p> <p>“0” indicates that no limit is imposed on number of attempts (except for what may be restricted by rate limits) and only the time interval applies.</p>  |
| Quarantine Time (min)               | <p>In the <b>Quarantine Time (min)</b> field, enter the time in minutes, a value from 1 to 1440. This field specifies the amount of time, in minutes, that a source IP address and port number is put on quarantine when it has a REGISTER requested with 403 response from S-CSCF and does not get a successful REGISTER within the specified time (or reaches the maximum attempts). When in quarantine, all messages received from that source IP address and port number are dropped. The maximum time limit is 24 hours.</p> <p>The value of this field has an interaction with P-CSCF Profile field “Backoff Interval for Improper REGISTER”. The PCSCF field, when used, directs the UE to avoid registering until one half of the specified time has expired.</p> <p>If the quarantine time specifies a value smaller than half of the backoff time, it indicates that the UE tries to send REGISTER requests while still in quarantine.</p> <p>If the quarantine time specifies a value larger than half the backoff time, it does not try to send REGISTER request until the quarantine is lifted; so quarantine time must not be much greater than half the backoff time to delay any unnecessary attempts to allow a REGISTER.</p> |

5 Click **OK**.

**Result:** A new Registration Failure Policy is added.

For more information on the parameters, see the topic “Registration Failure Policy” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision an Application Layer Policy

## Purpose

This procedure is used to provision an Application Layer Policy.

## Steps to provision an Application Layer Policy table

Perform the following steps at the Provisioning GUI:

**1** Select **IMS → SIP Tables**.

**Result:** The **SIP Tables** window is displayed.

In the left pane, expand the **Application Layer Policy** folder.

**Result:** The Application Layer Policy table is listed under the folder in the left pane.

If the folder is empty, add an Application Layer Policy table.

**2** Perform the following steps in the **SIP Tables** window to add, rename, or delete an Application Layer Policy table:

| If you want to...                                     | then...  |
|---|--|
| add an Application Layer Policy table,                | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add Application Layer Policy table</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <i>End of steps.</i> |
| modify (or rename) an Application Layer Policy table, | <ol style="list-style-type: none"><li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Rename Application Layer Policy table</b> window is displayed.</li><li>2. In the <b>Table Name</b> box, type a new table name.</li><li>3. Click <b>OK</b>.</li></ol> <i>End of steps.</i>   |

| If you want to...                              | then...  |
|--|--|
| delete an Application Layer Policy Rule table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p> |

- 3** Double-click the Application Layer Policy table. The Application Layer Policy table opens in the right pane. Perform the following steps to add, modify, or delete the Application Layer Policy table attributes:

| If you want to ...                                | Then ...   |
|---|--|
| add Application Layer Policy table attributes,    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Application Layer Policy</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>   |
| modify Application Layer Policy table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Application Layer Policy</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>    |
| delete Application Layer Policy table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> |

- 4** Provision the following parameters:

| Parameter          | Description  |
|--------------------|--|
| <b>Policy Id</b>   | Select the Application Layer Policy ID from the <b>Policy ID</b> list.           |
| <b>Description</b> | In the <b>Description</b> field, enter the Application Layer Policy description. |

| Parameter                      | Description  |
|--------------------------------|--|
| Registration Failure Policy ID | In the <b>Registration Failure Policy ID</b> field, select the index to Registration Failure Policy.<br>Zero indicates that there is no Registration Failure Policy to apply for this Application Layer Policy.<br><b>Note:</b> The value of zero does not apply when only one policy exists. However, zero is useful when multiple application layer policies are defined in future releases. |

- 5 Click **OK**.

**Result:** A new Application Layer Policy is added.

For more information on the parameters, see the topic “Application Layer Policy” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision a Security Gateway Profile

## Purpose

This procedure is used to provision a Security Gateway Profile.

## Steps to provision a Security Gateway Profile

Perform the following steps at the Provisioning GUI:

**1** Select **IMS → SIP Tables**.

**Result:** The **SIP Tables** window is displayed.

In the left pane, expand the **Security Gateway Profile** folder.

**Result:** The Security Gateway Profile table is listed under the folder in the left pane.

If the folder is empty, add a Security Gateway Profile table.

**2** Perform the following steps in the **SIP Tables** window to add, rename, or delete a Security Gateway Profile table:

| If you want to...                                    | then...   |
|--|---|
| add a Security Gateway Profile table,                | <ol style="list-style-type: none"> <li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add Security Gateway Profile table</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <i>End of steps.</i> |
| modify (or rename) a Security Gateway Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Rename Security Gateway Profile table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <i>End of steps.</i>   |

| If you want to...                             | then...  |
|---|--|
| delete a Security Gateway Profile Rule table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p> |

- 3 Double-click the Security Gateway Profile table. The Security Gateway Profile table opens in the right pane. Perform the following steps to add, modify, or delete the Security Gateway Profile table attributes:

| If you want to ...                                | Then ...   |
|---|--|
| add Security Gateway Profile table attributes,    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Security Gateway Profile</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>   |
| modify Security Gateway Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Security Gateway Profile</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol>    |
| delete Security Gateway Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p> |

- 4 In the **Profile Id** field, select a unique number.
- 5 In the **Description** field, enter a brief description .
- 6 In the **Flow Trusted Source Address Policy Id** field, select the value that you want to associate to this profile.

- 
- 7 In the **Flow Untrusted Source Address Policy Id** field, select the value that you want to associate to this profile.
- 
- 8 Select the **Aggregate Trusted Source Address Policy Id** that you intend to associate to this profile from the drop-down list.
- 
- 9 In the **Aggregate Untrusted Source Address Policy Id** field, select the value that you want to associate to this profile.
- 
- 10 In the **Application Layer Policy** field, select the Application Layer Policy ID that you want to associate to this profile.
- Note:** Value of zero indicates that no application layer policies are applied for this Security Gateway Profile.
- 
- 11 **Note:** The steps between [Step 11](#) and [Step 18](#) are relevant only if the integrated Security Gateway is used in the context of Signaling Firewall. The FEPH data must be added only if the Signaling Firewall is going to be used and the FEPH license is purchased.
- In the **Trusted Policy Id** field, select the FEPH policy Id that the FEPH should use for trusted flows.
- 
- 12 In the **Trusted Timeout (mins)** field, enter the trusted FEPH policy timeout. The range is 1 to 1440. The default value is 30.
- 
- 13 In the **Quarantine Policy Id** field, select the FEPH policy ID that the FEPH must use for flows that are under quarantine.
- 
- 14 In the **Quarantine Timeout (mins)** field, enter the quarantine FEPH policy timeout. The range is 1 to 1440. The default value is 30.
- 
- 15 In the **Default Inbound Policy Id** field, select the FEPH policy Id that the FEPH must use for the new (that is, untrusted) inbound flows.

- 16 In the **Default Inbound Policy Timeout (mins)** field, select the duration of time during which the **Default Inbound Policy Id** is valid for the new inbound flows.
- 17 In the **Default Outbound Policy Id** field, select the FEPH policy ID that the FEPH must use for new outbound flows (established by outbound packets).
- 18 In the **Default Outbound Policy Timeout (mins)** field, select the duration of time during which the **Default Outbound Policy Id** is valid for the new outbound flows.
- 19 In the **Remote IP Policy ID** field, select the appropriate instance of the Remote IP Policy.
- 20 Click **OK**.

**Result:** A new Security Gateway Profile is added.

For more information on the parameters, see the topic “Security Gateway Profile” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision support of digit analysis and normalization function

## Overview

### Purpose

This section provides information on the Digit Analysis rules and the procedures to provision support of Digit Analysis and Normalization Function.

**Note:** This feature is available only on 5400 LCP.

### Contents

|  |       |
|--|-------|
| Introduction to Digit Analysis (DA) tables | 5-95  |
| Digit Analysis (DA) Rules                  | 5-98  |
| Digit Analysis (DA) Rules -BGCF            | 5-105 |
| To provision a SIP Error Code table        | 5-106 |
| To provision an IMS Digit Table            | 5-110 |

# Introduction to Digit Analysis (DA) tables

## Overview

This topic describes the Digit Analysis (DA) tables.

### DA tables

The DA tables allow an operator to provision the matching strings, associate a number type for each matching string (an entry in the DA table), and define different operations for each matched string.

Each matched string can also be associated with a re-run DA table. The Re-run table provides a flexible mechanism to allow hierachal tables to be used, that can extend the number of entries (if needed) for DA functions and allow optimization of matching performances when the number of entries in the DA tables is large.

The DA tables are used to perform the following DA operations depending on the dialing plan used in the network.

- **Normalization of global numbers :** A global number refers to any phone number that can be normalized to E.164 international format.

Global numbers can be dialed in the following formats:

- National format or Local format (For example, 7-digit dialing in USA)
- with international dialing prefix (For example, 011 in US or 00 in France)
- in E.164 format (with a leading “+”)

The treatment for global numbers is to normalize (translate) them to E.164 international format. The translation rules are configured in the DA tables. In these tables, the rules are identified via the **Number Type** which can be “Local” or “National”.

- **Handling of invalid numbers :** Invalid numbers refer to unauthorized numbers, numbers with invalid syntax (minimum length, maximum length, authorized characters) or invalid ranges as defined by the customer. The control rules are configured in the DA tables. In these tables, the rules are identified via the **Number Type** which is “Invalid Destination”. When a dialed string does not match any entry in the DA table, the call will proceed as dialed to the next hop (ENUM query may be invoked or bypassed base on existing rules of 5450 ISC.).

For more information on provisioning the IMS Digit Analysis table, refer to “[To provision an IMS Digit Table](#)” (p. 5-110)

### Examples of DA table entries

The table below provides some examples for DA table entries.

| Match string | Number type         | Translate rule | Treatment | Note  |
|--------------|---------------------|----------------|-----------|---|
| 01XXXXXXX    | National            | +331XXXXXXX    |           | The dialed number 0198765432 completes to +33198765432  |
| 02XXXXXXX    | National            | +332XXXXXXX    |           | The dialed number 0298765432 completes to +33298765432  |
| 0262XXXXXX   | Local               | +262262XXXXXX  |           | The dialed number 0262123456 completes to +262262123456 |
| 0269XXXXXX   | Local               | +262269XXXXXX  |           | The dialed number 0269123456 completes to +262269123456 |
| 0594XXXXXX   | Local               | +594594XXXXXX  |           | The dialed number 0594123456 completes to +594594123456 |
| 0150XXXXXX   | Invalid Destination |                | 1         |   |
| 0600XXXXXX   | Invalid Destination |                | 1         |   |

**Notes:**

1. **Note :** Not all fields are shown in the table.

**Re-Run Digit table**

After a given digit translation, the new number may be optionally retranslated in a different table using the Re-Run Digit table setting, subject to the following limits and precautions.

- Re-Run Digit table is not allowed on the same table number.
- A maximum of 16 Re-Run Digit table executions is enforced per call.
- Care must be taken not to create a translations loop, that endlessly rematches or converts back and forth between a pair of complimentary digit strings.

## DA tables assignment

Each S-CSCF profile is provisioned with an index to a DA table. Each DA table entry can optionally have a re-run DA table assigned. Up to 16 re-runs are permitted per call.

Generally, each DA table that is pointed to by the S-CSCF profile corresponds to a dialing plan. Each dialing plan may have one or more country codes. If multiple dialing plans (or DA tables) are to be supported, then one way to support this would be to use multiple S-CSCF profiles, each corresponding to a dialing plan (DA table). When the S-CSCF instance is created, it needs to point to the S-CSCF profile. The DA table index is provisioned in the S-CSCF profile. For more information, refer to “[To provision an S-CSCF profile](#)” (p. 4-15)

## Number and size of DA tables

The DA function will support up to 2048 entries per DA table. Up to 256 DA tables can be configured on an IMS system, with a total of 10000 entries for all DA tables, whichever limit is reached first. Note that only one DA table is needed in a mono-country implementation (if we don't need to configure re-run table entries since re-run on the same table number is not allowed). For each DA table, the digit string that is used for matching and translation can have up to 24 digits.

# Digit Analysis (DA) Rules

## Overview

This topic describes the Digit Analysis rules.

## Matching Rules

The matching rules are as follows:

- The specific digits that may be matched are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 and “+”.
- The commonly used wildcard matches include the following:
  - N matches one digit with a value of 2-9
  - P matches one digit with a value of 0-1
  - X matches one digit of any value (this includes 0-9, “+”)
  - Y and Z have the same matching rules and priority as X. The wildcards Y and Z are used when multiple wildcards are needed in a digit string.
  - The form “@N@M” matches a range of digits. Refer to “[Range Match Rules](#)” ([p. 5-98](#))
  - The character “&” matches zero or more digits of any value.

**Note:** For the DA function, the only specific digits that may be matched include 0-9 and “+”. Consequently, wildcard X will match one digit of any value including 0-9 and “+”.

**Note:** The character “&” matches more than 24 digits.

**Note:** X is usually preferred over N in a match string, as N cannot be used in **Dialed Number Translate** (but X may be).

## Range Match Rules

The general form of a range match is some fixed initial digit string, followed by a range of digits (quantity) specified in the general form “@N@M” where:

- N - The minimum number of digits to follow
- M - The maximum number of digits to follow

The “range” digits are matched according to the wildcard rules for ‘X’ (0-9, “+”). The purpose of the range match is to represent, in one rule, a match of a fixed initial string, followed by a variable number of ‘X’ wildcard matches.

For example, 123@3@9 can be used to replace the following rules:

- 123XXX
- 123XXXX
- 123XXXXXX

- 123XXXXXX
- 123XXXXXXX
- 123XXXXXXXX
- 123XXXXXXXXX

This has the advantage of saving memory in real-time situations where a known initial digit string is followed by a variable quantity of digits. This is particularly useful for numbering plans that have variable-length geographic codes and/or subscriber numbers.

The following restrictions apply to the “@N@M” syntax:

- N and M represent integer values in the range 1 through 23
- N must be less than M
- One or more specific digits (For example, 0-9, “+”) must precede “@N@M”, and the sum of the length of prefixed string and the value of M must not exceed 23
- “@N@M” must be located at the end of the match string and nothing else will follow
- ‘&’ is not allowed in the same match string as “@N@M”
- Two “@N@M” match strings with the same prefix must not have overlapping lengths within a given table
- The “@N@M” syntax is only supported in a match string (not translation).

The table below gives some examples of the allowed and not allowed “@N@M” match strings with an explanation.

| Match String | Allowed?                        | Explanation  |
|--------------|---------------------------------|--|
| 1234@4@4     | No                              | The proper match to use is 1234XXXX.   |
| @2@3         | No                              | Ambiguous - “@N@M” must be preceded by some specific digits.   |
| &@2@3        | No                              | Ambiguous - “@N@M” must follow a match on one or more specific digits and will not be used in combination with “&”.    |
| X@2@3        | No                              | This is a degenerate form of @3@4 which is not allowed.  |
| 1@2@3&       | No                              | Ambiguous - “@N@M” must be the last part of the match string and may not be used in combination with the wildcard “&”. |
| 1234@3@5     | Not allowed in same digit table | There is an ambiguous overlap for “1234” followed by 4-5 more digits.  |
| 1234@4@7     |                                 |  |
| 1234@3@5     | Allowed in same digit table     | There is no ambiguity in these strings when used in the same digit table.  |
| 1234@6@7     |                                 |  |

The matching priority of "@N@M" is:

- "@N@M" has higher precedence than rules with '&' match character.
- "@N@M" has lower precedence than rules with specific number of 'X'(s).

If the match string includes a legal "@N@M" match, and the dialed translation contains the character "&", then the "&" stands for the portion of the digit string that matched the "@N@M". Any digit preceding the "@N@M" in the match must be explicitly included in the translation if it is required.

For example,

- Match string = 040@3@10
- Dial Translation = +4940&
- User dials = 0401234
- Digit analysis produces = +49401234

The "@N@M" match may be used in any digit table. However, care must be taken while applying this match. When used with the "Invalid Destination" number type, beware of unintended matches that would block valid calls.

## Matching Priority

The priority of digit string matching is assigned by sorting in digit order, and also most specific to least specific strings.

The sorted digit order from highest to lowest sort priority is as follows:

- Numeric: 9, 8, 7, 6, 5, 4, 3, 2, 1, 0
- Wildcard: N, P, X, Y, Z
- Miscellaneous digits: +
- Wildcard: &

Note that match strings are grouped together, by digit or wildcard. For example, all match strings that begin with 'N' come before all match strings that begin with 'X'. Within each grouping, the sorted order is applied progressively, digit by digit. Therefore, within the group of strings that begin with 'N', the string 'N5' has a higher priority than 'NX'.

## Priority Overlap

It is possible for digit table entries to partially overlap. When this happens, digit analysis chooses the entry that provides the most specific match.

The matching priority from highest to lowest is as follows:

- Specific digits (no wildcards) - Shorter specific strings have a higher priority than a longer string. For example, 911 has a higher priority than 9112.
- Wildcards of known length - For example, X has a higher priority than “&”.
  - 0XX has a higher priority than 0XXX (based on the string length).
  - A range match containing “@N@M” is interpreted as a set of matches with the corresponding number of “X” digits. However, a range of X has a lower priority than a specific quantity of X. For example, the following combination of matches shows the relative priority of range matches, from highest to lowest:

|             |
|-------------|
| 0123N&      |
| 0123XXXXXXX |
| 0123@2@3    |
| 0123@5@7    |
| 0123XX&     |
| 0123&       |

- 0X& has a higher priority than 0&
- 678& has a higher priority than 67&
- Wildcard string of unknown length and content (For example, &)

### Examples of Sorted Match Strings

The following digit strings illustrate how the concepts of Matching Priority and Priority Overlap apply to a set of digit strings.

The following strings are sorted from highest to lowest priority:

- 2003004567
- 1XX
- 1@2@4
- 1@6@9
- 1XX&
- NXX
- NXX123
- NXX1234567
- NXXX
- N&
- PXX123
- XXXXXXX

- +90&
- +XX
- &

### Wildcard Digits Behavior

The specific digits used in the examples are 0-9 and “+”. The behavior of the wildcard digits is as follows:

**Note:** If @N@M is in the match string and “&” in the Dialed Number Translate, “&” only stands for @N@M and not the entire match string. For example: When match string is 979@3@5, the dialed number translate is +1536&, and CdPN = 9790001, the result is +15360001 and not +15369790001, as “&” only stands for @N@M.

**Note:** This table is not applicable for BGCF. For more information on BGCF DA rules, see “[Digit Analysis \(DA\) Rules -BGCF](#)” (p. 5-105)

| Wildcard | Matched string behavior                         | Dialed # Translate behavior   | Notes   |
|----------|---|---|---|
| X        | Any digit 0-9, “+”                              | Corresponding X position in the match string  |   |
| Y and Z  | Same as X                                       | Corresponding Y (or Z) in the match string  | Used when wildcard digits matched must be moved to different position in Dialed Number Translate. |
| P        | 0 or 1  | Not allowed   | P is only used in match string, not in translate string.  |
| N        | 2-9   | Not allowed   | N is only used in match string, not in translate string.  |
| &        | Zero or more digits, any value (digit 0-9, “+”) | If “&” occurs in the match string, then it stands for all the digits matched by “&”. If “&” does not occur in the match string, then it stands for the entire match string. |   |

### Examples

In the following examples, the calling phone is “+19742210000” and the destination is “+19742210005”. Country code 1 is used within the examples.

| Match string | Translate rule | Call and result   |
|--------------|----------------|---|
| NXXXXXX      | +1974&         | Dialed number 2210005, call completes to +19742210005. This is because "&" matches N and X.   |
| 1XXXXXXXX    | +1974&         | Dialed number 12210005, call fails. Constructed string is +197412210005. This is because the "&" matches the whole string including specific and wildcard digits.     |
| 1NXXXXXX     | +1974NXXXXXX   | Rejected on input to GUI. This is because N may not be used in Dialed Number translate.   |
| 1NXXXXXX     | +1974XXXXXXX   | Rejected on input to GUI. This is because N in the match string may not be replaced by X in the Dialed Number translate string.                                       |
| 1XXXXXX      | +1974XXXXXXX   | Rejected on input to GUI. This is because the number of X in match string must agree with the number in Dialed Number translate.                                      |
| 1XXXXXXX     | +1974XXXXXXX   | Dial 12210005, call completes to +19742210005.  |
| 0X           | +1974221000X   | Dial 05 completes to +19742210005. Dial 01 completes to +19742210001.   |
| 3XXXX3       | +1974221XXXX   | Dial 300053 completes to +19742210005. This is because the matched XXXX can be in the middle of the string.   |
| XXXXYYY      | +1974YYYXXXX   | Dial 0005221, call completes to +19742210005. This is because X and Y can be used to modify the order of digits in the wildcards. In this case XXXX=0005 and YYY=221. |
| 1&           | +1974221&      | Dial 10005, call completes to +19742210005. This is because "&" matches "&"   |
| 1&           | +1974221X      | Rejected on input to GUI. This is because exactly one digit cannot be substituted for cases where "&" would represent either none or more than one digit.             |

| Match string | Translate rule | Call and result  |
|--------------|----------------|--|
| N&           | &              | Dial 289 translates to 89. This is because “&” exactly matches “&” (N is not matched and is discarded in this case).   |
| P11          | 19742210005    | Dialing 011 or 111 completes to +19742210005. Dialing 311 fails (no match). This is because P matches 0 or 1.  |
| Z (or Y)     | 1974221005     | Dialing any single digit (for example, 0-9 or *) completes to +1974221005. This is because Z or Y match any digit like X.  |
| 1PX          | +197422100&    | Dial 105 routes to +197422100105 (failure). This is because the “&” matches the entire 1PX.  |
| 1XXX777XXXX  |                | Rejected on input to GUI. This is because wildcards of the same character (X) must be grouped together. Note: The alternative is to specify this string as 1XXX777YYYY.  |
| 040@3@5      | +4940&         | <p>This is a variable length digit match. If the user dials 040 followed by 3-5 digits, it matches this translation. The "&amp;" in Dialed Number Translate matches the 3-5 digits following 040. So if the user dials 0401234, the result is +49401234.</p> <p>Note that this translation is a short-hand for creating multiple match strings:</p> <ul style="list-style-type: none"> <li>• 040XXX</li> <li>• 040XXXX</li> <li>• 040XXXXX</li> </ul> <p>The variable length match saves memory and execution time compared to the three separate matches. This is particularly useful for the numbering plans that have variable-length geographic codes and/or subscriber numbers.</p> |

# Digit Analysis (DA) Rules -BGCF

## Overview

This topic describes the Digit Analysis (DA) rules applicable only for the BGCF component.

### Matching rules

The BGCF is provisioned with DA tables to match the digits received in the incoming message and based on the matching results a routing decision is made. The matching rules are applied for dialed digits, CIC matching and Called Party Pattern matching.

The digits supported on the DA Table are “**0-9**” , hex digits “**A-F**” or “**a-f**” , “#” , “\*” , “&” and “x”. “x” is the single digit wild card and “&” is a wild card with one or more digits.

The DA table is stored and sorted so that the matching function can be performed as listed below:

- Best match for the longest string.
- Exact match preferred over wild card match.

For example, if “0” and “0&” are provisioned, and if the dialed digit is a “0”, then “0” is matched instead of “0&”.

#### Note:

- The wildcard character “&” matches one or more digits and is considered as a place holder for one or more digits. No digits are allowed after “&” . For example, “123&” is allowed, but “123&5” is not allowed.
- The wildcard character “x” is considered as a placeholder for a single digit and has a higher preference over the wildcard character “&” .
- Multiple wildcard characters in a string are allowed. For example, “123xx67&”.

# To provision a SIP Error Code table

## Purpose

This procedure is used to provision a SIP Error Code table.

## Description

The SIP Error Code table is a general purpose table. Digit Analysis makes use of this general purpose table. When the system encounters a match for an ID in this table, it will add a “Status Code” (corresponding to Error Code) and a “Reason Phrase” (corresponding to Error Code Phrase) to the top line in the SIP error response.

## Before you begin

Digit Analysis will only use this table to handle the “**Number Type = Invalid Destination**” in the E.164 Table and will return the specified **Error Code** and **Error Code Phrase** to the customer who dialed the Invalid Destination.

This procedure is performed at the Provisioning GUI.

## Steps to provision a SIP Error Code table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS → SIP Tables**.

**Result:** The **SIP Tables** window is displayed.

---

- 2 In the left pane, expand the **SIP Error Code Table** folder.

**Result:** The SIP Error Code Table tables are listed under the folder in the left pane.

If the folder is empty, add a SIP Error Code table.

Perform the following steps in the **SIP Tables** window to add, rename, or delete a SIP Error Code table :

| If you want to ...             | then ...  |
|--------------------------------|---|
| add a SIP Error Code table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/> <b>Result:</b> The <b>Add SIP Error Code Table table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a SIP Error Code table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/> <b>Result:</b> The <b>Rename SIP Error Code Table table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a SIP Error Code table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a SIP Error Code table, ensure that no table entries are in use.</p> <p><i>End of steps</i></p>  |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the SIP Error Code table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **SIP Tables - SIP Error Code Table** window to add, modify, or delete the SIP Error Code table attributes:

| If you want to ...                        | then ...   |
|---|--|
| add the SIP Error Code table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Error Code</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a SIP Error Code table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Error Code</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a SIP Error Code table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>              |

- 5 Provision the following parameters:

| Parameter                | Provisioning  |
|--------------------------|---|
| <b>ID</b>                | Select the ID for the drop-down list.                 |
| <b>Error Code</b>        | Enter a 3-digit numeric value for the SIP Error Code. |
| <b>Error Code Phrase</b> | Enter a description for the SIP Error Code.           |

For more information on the parameters, see the topic **SIP Error Code** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The SIP Error Code table attributes are provisioned successfully.

END OF STEPS

---

# To provision an IMS Digit Table

## Purpose

This procedure is used to provision an IMS Digit Table.

## Steps to provision an IMS Digit Table

Perform the following steps at the Provisioning GUI:

- 1 Select **Routing → Digit Tables**.

**Result:** The **Digit Tables** window is displayed.

- 2 In the left pane, expand the **IMS Digit Table** folder.

**Result:** The IMS Digit Table tables are listed under the folder in the left pane.

If the folder is empty, add an IMS Digit Table.

Perform the following steps in the **Digit Tables** window to add, rename, or delete an IMS Digit Table:

| If you want to ...         | then ...   |
|----------------------------|--|
| add an IMS Digit Table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add IMS Digit Table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> drop-down list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename an IMS Digit Table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Digit Table Designation</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |

| If you want to ...         | then ...  |
|----------------------------|---|
| delete an IMS Digit Table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an IMS Digit Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the IMS Digit Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **Digit Tables** window to add, modify, or delete the IMS Digit Table attributes:

| If you want to ...                    | then ...  |
|---------------------------------------|---|
| add the IMS Digit Table attributes,   | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.</li> </ol> <p><b>Result:</b> The <b>Digit Tables</b> window is displayed.</p> <ol style="list-style-type: none"> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify an IMS Digit Table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.</li> </ol> <p><b>Result:</b> The <b>Digit Tables</b> window is displayed.</p> <ol style="list-style-type: none"> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                    | then ...   |
|---------------------------------------|--|
| delete an IMS Digit Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>  |
| import an IMS Digit Table from file,  | <p>An IMS Digit table can be imported from file.<br/>The <b>Import Table</b> option is used to read a <i>.csv</i> file and create a table with those entries.</p> <p>To import an IMS Digit table,</p> <ol style="list-style-type: none"> <li>At the Provisioning GUI, click <b>Digit Tables</b>.</li> <li>Expand the <b>IMS Digit Table</b> folder.</li> <li>Right-click the desired entry and select <b>Import Table</b> from the menu.<br/><b>Result :</b> The <b>Import Digit Table File</b> window is displayed.</li> <li>Browse to the location and select the desired file with a <i>.csv</i> extension.</li> <li>Click <b>Open</b>.</li> </ol>         |
| export an IMS Digit Table to file,    | <p>The IMS Digit Table can be exported to file.<br/>The <b>Export Table</b> option is used to generate a <i>.csv</i> (common separated value) file.</p> <p>To export an IMS Digit table,</p> <ol style="list-style-type: none"> <li>At the Provisioning GUI, click <b>Digit Tables</b>.</li> <li>Expand the <b>IMS Digit Table</b> folder.</li> <li>Right-click the desired entry and select <b>Export Table</b> from the menu.<br/><b>Result :</b> The <b>Export Digit Table File as</b> window is displayed.</li> <li>Browse to the desired location where you want to save the file ( with a <i>.csv</i> extension).</li> <li>Click <b>Save</b>.</li> </ol> |

**5** Provision the following parameters:

| Parameter                    | Provisioning  |
|------------------------------|---|
| <b>Enable</b>                | This parameter specifies whether or not the digit table record is to be downloaded to the IMS Nodes/Cards.  |
| <b>Digit Table Operation</b> | This parameter defines the operation that will be applied to the matched digit.<br>The default value is “Translation”.<br>“Translation” means that the dialed number will be translated using the pattern provided in the <b>Dialed Number Translate</b> field. |
| <b>String to Match</b>       | This parameter specifies the received number that will be used to match with the <b>Match String</b> field.   |
| <b>Match String</b>          | This parameter provides the pattern that the system will use to match against the dialed number.  |

| Parameter                      | Provisioning  |
|--------------------------------|---|
| <b>Number Type</b>             | <p>This parameter specifies the type of call. The following options can be selected:</p> <ul style="list-style-type: none"> <li>• <b>Local</b> : This option indicates that the dialed number will be treated as a local number. Local numbers are unique only within a certain geographical area or a certain part of the telephone network. When the system receives this indication, it will translate the dialed number according to the <b>Match String</b> and <b>Dialed Number Translate</b> fields. The system will also add “user=phone” to the Request-URI (if it is an SIP URI).</li> <li>• <b>National</b> : This option indicates that the dialed number will be treated as a national number. National numbers are designated to be used within the country. When the system receives this indication, it will translate the dialed number according to the <b>Match String</b> and <b>Dialed Number Translate</b> fields. The system will also add “user=phone” to the Request-URI (if it is an SIP URI). <b>Note</b> : Currently the national and local numbers are treated similarly.</li> <li>• <b>Invalid Destination</b> : This parameter indicates that the dialed number will be treated as an Invalid Number.</li> </ul> |
| <b>Dialed Number Translate</b> | <p>When left blank, this field indicates that there is no change to the dialed number. This field specifies the pattern the system will use to translate a number. When the system receives the dialed number and it matches the <b>Match String</b> field, the system will translate the dialed number according to the pattern specified in the <b>Dialed Number Translate</b> field.</p>   |

| Parameter                 | Provisioning  |
|---------------------------|---|
| <b>Re-run Digit Table</b> | <p>This field specifies the digit table that will run next. This field contains a list of all the available Digit Table IDs.</p> <p>If the pattern designated by the <b>Match String</b> field does not provide the full translation pattern, a Re-run Digit Table can be specified. It will contain the table number where the remaining portion of the pattern matching is provided. The Re-run digit table cannot be specified to the digit table by itself.</p> |
| <b>SIP Error Code ID</b>  | <p>This field specifies the SIP error response that will be sent when the Number Type is set to Invalid destination. A check is performed on this field to ensure that a valid ID is selected when the <b>Number Type</b> is set to “Invalid Destination”. The SIP Error Code Id is provided by the SIP Error Code Table. For more information on SIP Error Code Table, refer to “<a href="#">To provision a SIP Error Code table</a>” (p. 5-106)</p>               |

For more information on the parameters, see the topic **IMS Digit Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

---

**6** Click **OK**.

**Result:** The IMS Digit Table attributes are provisioned successfully.

END OF STEPS

---

# To provision ICSI

## Overview

### Purpose

This section provides the procedures for ICSI provisioning.

### Contents

|                              |       |
|------------------------------|-------|
| To provision an ICSI profile | 5-117 |
|------------------------------|-------|

# To provision an ICSI profile

## Purpose

This procedure is used to provision an ICSI profile.

## Before you begin

The following SDP media information has to be provisioned:

- SDP media codec
- SDP media component policy
- SDP media subscription profile

To provision the SDP media settings, Refer to “[To provision SDP media](#)” (p. 4-6)

## System requirements

Provisioning GUI connection.

## Steps to provision an ICSI Profile table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS → IMS Components → SCSCF Tables**.

**Result:** The **SCSCF Tables** window is displayed.

---

- 2 In the left pane, expand the **ICSI Profile** folder.

**Result:** The ICSI Profile tables are listed under the folder in the left pane.

If the folder is empty, add an ICSI Profile table.

Perform the following steps in the **SCSCF Tables** window to add, rename, or delete an ICSI Profile table :

| If you want to ...            | then ...   |
|-------------------------------|--|
| add an ICSI Profile table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>SCSCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename an ICSI Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>SCSCF Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |
| delete an ICSI Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an ICSI Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>   |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the ICSI Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **SCSCF Tables** window to add, modify, or delete the ICSI Profile table attributes:

| If you want to ...                       | then ...   |
|--|--|
| add the ICSI Profile table attributes,   | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify an ICSI Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete an ICSI Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p>             |

- 5 Provision the following parameters:

| Parameter       | Provisioning                              |
|-----------------|---|
| ICSI Profile ID | The ICSI Profile Ids range from 1 to 100. |

| Parameter                               | Provisioning   |
|---|--|
| <b>ICSI Value</b>                       | <p>The ICSI value should not be null and its maximum length is 256. This value is used to match with one of the values of the "List of Service IDs" data that is provisioned to the subscriber in the HSS.</p> <p><b>Note:</b> The S-CSCF receives the "List of Service IDs" as a part of the Service profile data during registration.</p>  |
| <b>Service Must Use ICSI</b>            | <p>Enable the <b>Service Must Use ICSI</b> check box to include the P-Asserted-Identity header in the outgoing request.</p>  |
| <b>Content Type List</b>                | <p>The <b>Content Type List</b> specifies the possible values of a Content-Type header that the S-CSCF shall use to validate against a received SIP request.</p> <p>To add a Content-Type value,</p> <ol style="list-style-type: none"> <li>Under <b>Content Type List</b>, click <b>Add</b>.</li> <li>Add the Content-Type value in the dialog box that appears. Click <b>OK</b>.</li> </ol> <p>To delete a Content-Type value, select the desired value in the <b>Content Type List</b> and click <b>Delete</b>.</p> |
| <b>Media Component Policy Treatment</b> | <p>One of the following three values can be selected:</p> <ul style="list-style-type: none"> <li><b>Allow</b> - This means that only the listed policies are allowed (the received SIP message has to match one of them.)</li> <li><b>Require</b> - This means that all the listed policies must be met for the received SIP message</li> <li><b>Disallow</b> - This means that the listed policies are blocked.</li> </ul>  |

| Parameter                     | Provisioning  |
|-------------------------------|---|
| <b>Media Component Policy</b> | <p>The <b>Media Component Policy</b> specifies the SDP policies that the S-CSCF uses for validation. For validation, the S-CSCF uses the media description part of the received SDP in SIP requests during session establishment and modification.</p> <p>To add a SDP Media Component policy,</p> <ol style="list-style-type: none"><li>Under <b>Media Component Policy</b>, click <b>Add</b>.</li><li>In the dialog box that appears, select the Media Component Policy from the <b>Media Component policy</b> list.</li><li>Select the appropriate ID.</li><li>Click <b>OK</b>.</li></ol> <p>To delete a SDP Media Component policy,</p> <ul style="list-style-type: none"><li>Select the desired value in the <b>Media Component policy</b> list and click <b>Delete</b>.</li></ul> |

For more information on the parameters, see the topic **ICSI Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click **OK**.

**Result:** The ICSI Profile table attributes are provisioned successfully.

END OF STEPS

---

# To provision bearer statistics collection on the iAGCF

## Overview

### Purpose

This section provides the procedure to provision support of Bearer Statistics Collection on the iAGCF.

### Contents

|   |       |
|---|-------|
| Support collecting Bearer statistics at AGCF from Access GW | 5-123 |
|---|-------|

# Support collecting Bearer statistics at AGCF from Access GW

## Overview

The feature “Support collecting Bearer statistics at AGCF from Access GW” supports collection of bearer statistics from the AGW (ISAM and Litespan) and passing them to CCF via the Rf interface.

During call teardown, the AGCF sends a Subtract message to the AGW with the Audit Statistics Descriptor. This causes the AGW to send back the required Bearer statistics data for the Context. This is then relayed to CCF in the ACR[Event] message.

# To provision the support of session and bandwidth limits per enterprise/PBX

## Overview

### Purpose

This section provides the procedure to provision the support of session and bandwidth limits per enterprise/PBX.

### Contents

|   |       |
|---|-------|
| To provision a Virtual Group profile          | 5-125 |
| To provision a Service Level Policy           | 5-129 |
| To provision the IBC-A VG Policy              | 5-133 |
| To provision a VG and Service Mapping Profile | 5-137 |

# To provision a Virtual Group profile

## Purpose

This topic describes the steps to provision a Virtual Group profile.

## Before you begin

If you are deleting a Virtual Group profile, ensure that the profile is not configured in the **Virtual Group and Service Mapping** table.

## Steps to provision a Virtual Group profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → VG Session BW Control**.

**Result:** The **VG Session&BW control** window is displayed.

- 2 In the left pane, expand the **Virtual Group Profile** folder.

**Result:** The Virtual Group Profile tables are listed under the folder in the left pane.

If the folder is empty, add a Virtual Group profile table.

Perform the following steps in the **VG Session&BW control** window to add, rename, or delete a Virtual Group profile table :

| If you want to ...                 | then ...   |
|------------------------------------|--|
| add a Virtual Group profile table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW control</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                    | then ...   |
|---------------------------------------|--|
| rename a Virtual Group profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW control</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a Virtual Group profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Virtual Group profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>         |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the Virtual Group profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **VG Session&BW control** window to add, modify, or delete the Virtual Group profile table attributes:

| If you want to ...                              | then ...   |
|---|--|
| add the Virtual Group profile table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW control</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                               | then ...   |
|--|--|
| delete a Virtual Group profile table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter                        | Provisioning   |
|----------------------------------|--|
| <b>Virtual Group Member ID</b>   | Select a unique number from the <b>Virtual Group Member ID</b> drop-down list.   |
| <b>Component Type</b>            | Select the 5450 ISC component for which this profile is applicable from the <b>Component Type</b> drop-down list.  |
| <b>Match Type</b>                | Select the appropriate entry from the <b>Match Type</b> drop-down list.  |
| <b>Virtual Group Member Type</b> | <p>Select the virtual group criterion for associating the call session to the virtual group from the <b>Virtual Group Member Type</b> drop-down list.</p> <p>The available options:</p> <ul style="list-style-type: none"> <li>• Destination Trunk Group<br/><b>Note:</b> The destination trunk group identifier, if present, is found in parameters of the Request-URI in a SIP request.</li> <li>• Domain</li> <li>• IP address</li> <li>• Pr-Access-Network-Info</li> <li>• PrID</li> </ul> <p>The default value is Domain.</p> |
| <b>IP Address Type</b>           | Select the appropriate entry from the <b>IP Address Type</b> drop-down list.   |

| Parameter                   | Provisioning  |
|-----------------------------|---|
| <b>Netmask</b>              | Enter the IPv4 or IPv6 netmask in the <b>Netmask</b> field.   |
| <b>Virtual Group Member</b> | Enter the value to be associated with the member of this profile in the <b>Virtual Group Member</b> field.  |
| <b>Trunk Group Label</b>    | In the <b>Trunk Group Label</b> field, enter the string that appears after the “tgrp=” part of the parameter in the Request-URI.<br><br>This field is available only when the virtual group member type is Destination Trunk Group.   |
| <b>Trunk Context</b>        | In the <b>Trunk Context</b> field, enter the string that appears after the “trunk-context=” part of the parameter in the Request-URI.<br><br><b>Note:</b> For virtual group member type of Destination Trunk Group, the combination of "Trunk Group Label" and "Trunk Context" must be unique for each entry. This field is available only when the virtual group member type is Destination Trunk Group. |

For more information on the parameters, see the topic **VG Profile Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click **OK**.

**Result:** The Virtual Group profile table attributes are provisioned successfully.

END OF STEPS

---

# To provision a Service Level Policy

## Purpose

This topic describes the steps to provision a Service Level Policy.

## Before you begin

If you are deleting a Service Level Policy, ensure that the profile is not configured in the **Virtual Group and Service Mapping** table.

## Steps to provision a Service Level Policy table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → VG Session BW Control**.

**Result:** The **VG Session&BW Control** window is displayed.

- 2 In the left pane, expand the **Service Level Policy** folder.

**Result:** The Service Level Policy tables are listed under the folder in the left pane.

If the folder is empty, add a Service Level Policy table.

Perform the following steps in the **VG Session&BW Control** window to add, rename, or delete a Service Level Policy table :

| If you want to ...                | then ...   |
|-----------------------------------|--|
| add a Service Level Policy table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW Control</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                   | then ...   |
|--------------------------------------|--|
| rename a Service Level Policy table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW Control</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a Service Level Policy table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Service Level Policy table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>          |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the Service Level Policy table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **VG Session&BW Control** window to add, modify, or delete the Service Level Policy table attributes:

| If you want to ...                             | then ...   |
|--|--|
| add the Service Level Policy table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW Control</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                              | then ...   |
|---|--|
| modify a Service Level Policy table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW Control</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol> |
| delete a Service Level Policy table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.<br/><i>End of steps.</i></li> </ol>                             |

**5** Provision the following parameters:

| Parameter                      | Provisioning   |
|--------------------------------|--|
| <b>Service Level Policy ID</b> | Select a unique number from the <b>Service Level Policy ID</b> drop-down list.   |
| <b>Service Description</b>     | Enter a brief description in the <b>Service Description</b> field.   |
| <b>Max Incoming Sessions</b>   | Enter the maximum number of incoming sessions to be allowed for the virtual group in the <b>Max Incoming Sessions</b> field, or select the <b>Allow All Incoming Sessions</b> check box.         |
| <b>Max Outgoing Sessions</b>   | Enter the maximum number of outgoing sessions to be allowed for the virtual group in the <b>Max Outgoing Sessions</b> field, or select the <b>Allow All Outgoing Sessions</b> check box.         |
| <b>Max Incoming Bandwidth</b>  | Enter the maximum allowed bandwidth for the incoming call sessions of the virtual group in the <b>Max Incoming Bandwidth</b> field, or select the <b>Allow All Incoming Bandwidth</b> check box. |

| Parameter                     | Provisioning   |
|-------------------------------|--|
| <b>Max Outgoing Bandwidth</b> | Enter the maximum allowed bandwidth for the outgoing call sessions of the virtual group in the <b>Max Outgoing Bandwidth</b> field, or select the <b>Allow All Outgoing Bandwidth</b> check box. |

For more information on the parameters, see the topic **Service Profile Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 6 Click **OK**.

**Result:** The Service Level Policy table attributes are provisioned successfully.

END OF STEPS

# To provision the IBC-A VG Policy

## Purpose

This procedure describes the steps to provision the IBC-A VG Policy

## Steps to provision a IBC-A VG Policy table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → VG Session BW Control**.

**Result:** The **VG Session&BW Control** window is displayed.

- 2 In the left pane, expand the **IBC-A VG Policy** folder.

**Result:** The IBC-A VG Policy tables are listed under the folder in the left pane.

If the folder is empty, add a IBC-A VG Policy table.

Perform the following steps in the **VG Session&BW Control** window to add, rename, or delete a IBC-A VG Policy table :

| If you want to ...              | then ...   |
|---------------------------------|--|
| add a IBC-A VG Policy table,    | <ol style="list-style-type: none"> <li>1 Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW Control</b> window is displayed.</li> <li>2 From the <b>Table Number</b> list, select the table number.</li> <li>3 In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4 Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a IBC-A VG Policy table, | <ol style="list-style-type: none"> <li>1 Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW Control</b> window is displayed.</li> <li>2 In the <b>Table Name</b> box, type a new table name.</li> <li>3 Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |

| If you want to ...              | then ...   |
|---------------------------------|--|
| delete a IBC-A VG Policy table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a IBC-A VG Policy table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the IBC-A VG Policy table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **VG Session&BW Control** window to add, modify, or delete the IBC-A VG Policy table attributes:

| If you want to ...                         | then ...   |
|--|--|
| add the IBC-A VG Policy table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW Control</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a IBC-A VG Policy table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW Control</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                         | then ...  |
|--|---|
| delete a IBC-A VG Policy table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter  | Provisioning   |
|--|--|
| <b>IBC-A VG Policy ID</b>                            | In the <b>IBC-A VG Policy ID</b> field, select the instance of IBC-A VG Policy.  |
| <b>IBC-A VG Policy Description</b>                   | In the <b>IBC-A VG Policy Description</b> field, enter the description.  |
| <b>Core Next Hop for Registration</b>                | In the <b>Core Next Hop for Registration</b> field, select a non-zero value to specify an IBC Route Profile that is used to determine the next hop towards the core network for REGISTER requests. When zero, the existing IBC-A Profile field of the same name is used instead.                       |
| <b>Access Next Hop for Non-Registration Requests</b> | In the <b>Access Next Hop for Non-Registration Requests</b> field, select a non-zero value to specify an IBC Route Profile that is used to determine the next hop towards the access network for non- REGISTER requests. When zero, the existing IBC-A Profile field of the same name is used instead. |
| <b>Core Next Hop for Non-Registration Requests</b>   | In the <b>Core Next Hop for Non-Registration Requests</b> field, select a non-zero value to specify an IBC Route Profile that is used to determine the next hop towards the core network for non- REGISTER requests. When zero, the existing IBC-A Profile field of the same name is used instead.     |

For more information on the parameters, see the topic **IBC-A VG Policy** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The IBC-A VG Policy table attributes are provisioned successfully.

END OF STEPS

---

# To provision a VG and Service Mapping Profile

## Purpose

This topic describes the steps to provision a VG and Service Mapping Profile.

## Before you begin

To provision a VG and Service Mapping Profile, ensure that the Virtual Group profile, Service Level policy and the SDP profile are configured before you start this procedure.

To configure these profiles, refer “[Provision the support of session and bandwidth limits per enterprise/PBX](#)” (p. 1-60).

## Steps to provision a VG and Service Mapping Profile table

Perform the following steps at the Provisioning GUI:

- 1** Select **IMS → VG Session BW Control**.

**Result:** The **VG Session&BW Control** window is displayed.

- 2** In the left pane, expand the **VG and Service Mapping Profile** folder.

**Result:** The VG and Service Mapping Profile tables are listed under the folder in the left pane.

If the folder is empty, add a VG and Service Mapping Profile table.

Perform the following steps in the **VG Session&BW Control** window to add, rename, or delete a VG and Service Mapping Profile table :

| If you want to ...                          | then ...   |
|---|--|
| add a VG and Service Mapping Profile table, | <ol style="list-style-type: none"> <li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW Control</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                             | then ...  |
|--|---|
| rename a VG and Service Mapping Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW Control</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a VG and Service Mapping Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a VG and Service Mapping Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the VG and Service Mapping Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **VG Session&BW Control** window to add, modify, or delete the VG and Service Mapping Profile table attributes:

| If you want to ...                                       | then ...   |
|--|--|
| add the VG and Service Mapping Profile table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW Control</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

**Manage services**

*To provision the support of session and bandwidth limits per enterprise/PBX*

To provision a VG and Service Mapping Profile

| If you want to ...  | then ...  |
|---|---|
| modify a VG and Service Mapping Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>VG Session&amp;BW Control</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a VG and Service Mapping Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                             |

**5 Provision the following parameters:**

| Parameter                      | Provisioning  |
|--------------------------------|---|
| <b>Virtual Group ID</b>        | Select a virtual group profile from the <b>Virtual Group ID</b> drop-down list.   |
| <b>Mapping Description</b>     | Enter a brief description in the <b>Mapping Description</b> field.  |
| <b>Service Level Policy ID</b> | Select the Service level policy ID to be associated with the virtual group from the <b>Service Level Policy ID</b> drop-down list.                  |
| <b>SDP Policy Index</b>        | Select the Session Description Protocol profile ID to be associated with the virtual group from the <b>SDP Policy Index</b> drop-down list.         |
| <b>Sip Error Response Code</b> | Select the response code to be sent to the subscriber/peer network if the call is rejected, from the <b>Sip Error Response Code</b> drop-down list. |

For more information on the parameters, see the topic **Mapping Profile Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The VG and Service Mapping Profile table attributes are provisioned successfully.

---

END OF STEPS

---

# To provision signaling firewall

## Overview

### Purpose

This section provides the procedures to provision the Signaling Firewall, previously known as Secure External Access Lockout (SEAL).

### Contents

|  |       |
|--|-------|
| To provision FEPH Flow Policy                    | 5-142 |
| Provision an Aggregate Packet Policy             | 5-147 |
| Provision an Aggregate Flow Policy               | 5-150 |
| Provisioning task flow for hardware acceleration | 5-151 |
| Provision an Aggregate Policy Assignment         | 5-154 |
| To provision an IPsec Parameters table           | 5-155 |

# To provision FEPH Flow Policy

## Purpose

This procedure describes the steps to provision a Flow Policy.

## Before you begin

Six records of default flow policies are automatically generated. The descriptions of these policies indicate the configuration purpose. The parameters within the user-defined policies can be modified as required.

**Note:** The maximum allowed policies are 255

The Flow Policy ID ranges are defined as follows:

- IDs 1-100 are reserved for system default policies and are not allowed to be changed, inserted, or deleted.
- IDs 101 - 255 are custom policies and can be inserted, changed, and deleted.

To affect a new custom policy, a new policy ID must be created and then it must be assigned to the Security Gateway Profile (or AGCF profile for H.248) to replace a system default policy.

- By default, three policies with IDs 1, 2, 3 are created for SIP usage, and three policies with IDs 11, 12, and 13 are created for H.248 usage:

ID 1, and 11 are the quarantine policies.

ID 2, and 12 are policies for new inbound-initiated flows from individual endpoints.

ID 3, and 13 are policies for new outbound-initiated flows and registered endpoint.

| Flow Policy ID | Description                  | Inbound Large Packet Rate Limit | Inbound Small Packet Rate Limit | Minimum UDP Datagram Size | Minimum Fragment Size | SIP Inspection |
|----------------|------------------------------|---------------------------------|---------------------------------|---------------------------|-----------------------|----------------|
| 1              | SIP Quarantine Default       | Drop all                        | drop all                        | 60                        | 1000                  | Yes            |
| 2              | SIP Inbound Default          | 4                               | 2                               | 60                        | 1000                  | Yes            |
| 3              | SIP Outbound/Trusted Default | 100                             | 2                               | 60                        | 1000                  | Yes            |
| 11             | H248 Quarantine Default      | Drop all                        | Drop all                        | 60                        | 1000                  | No             |
| 12             | H248 Inbound Default         | 4                               | 2                               | 60                        | 1000                  | No             |

| Flow Policy ID | Description                         | Inbound Large Packet Rate Limit | Inbound Small Packet Rate Limit | Minimum UDP Datagram Size | Minimum Fragment Size | SIP Inspection |
|----------------|-------------------------------------|---------------------------------|---------------------------------|---------------------------|-----------------------|----------------|
| 13             | H248<br>Outbound/Trusted<br>Default | 100                             | 2                               | 60                        | 1000                  | No             |

Whenever a Flow Table main policy is installed, the FEPH marks/unmarks the flow as transient as follows:

- If the Flow Table entry timeout is set to  $\geq 600$  seconds, then the flow is marked as NOT transient.
- Else, the flow is marked as transient.

### Steps to provision a Flow Policy table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → FEPH Tables → Flow Policy**.

**Result:** The **Flow Policy** window is displayed.

- 2 Double-click the table to open the list of profiles defined for the table.

You can modify the attributes of existing profiles.

- 3 Perform the following steps at the **FEPH Flow Policy** window to modify the Flow Policy attributes:

| If you want to ...                     | then ...   |
|--|--|
| modify a Flow Policy table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes → Modify Table Attributes</b>.<br/><b>Result:</b> The <b>FEPH Flow Policy</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

**4** Provision the following parameters:

| Parameter  | Provisioning   |
|--|--|
| <b>Profile ID</b>                                | Select a unique ID for the flow policy.  |
| <b>Description</b>                               | Type a descriptive name for the flow policy.   |
| <b>Inbound Large Packet Rate Limit (per sec)</b> | <p>Select the number of large packets that are allowed to be received per second from a source IP address and port number.</p> <p>A large packet is a packet with a frame size of greater than or equal to 300 octets.</p> <p><b>Note:</b> The value “<b>Drop all</b>” indicates that the FEPH does not forward any applicable packets, and a value of “<b>No limit</b>” indicates that the FEPH does not impose a rate limit.</p> |
| <b>Inbound Small Packet Rate Limit (per sec)</b> | <p>Select the number of small packets that are allowed to be received per second from a source IP address and port number.</p> <p>A small packet is any packet with a frame size of less than 300 octets.</p> <p><b>Note:</b> The value “<b>Drop all</b>” indicates that the FEPH does not forward any applicable packets, and a value of “<b>No limit</b>” indicates that the FEPH does not impose a rate limit.</p>              |

| Parameter                        | Provisioning   |
|----------------------------------|--|
| <b>Minimum UDP Datagram Size</b> | <p>Type the minimum allowed UDP datagram size. The range varies from 60 to 1500. The default value is 60. Choose an appropriate value based on the type of UDP traffic that is expected or allowed from external sources.</p> <p><b>Note:</b> The UDP datagram size is the size of an Ethernet frame that carries the UDP datagram which includes the Ethernet header, the IP header, the transport header, the payload and the padding. Padding is inserted when the Ethernet frame size is less than the minimum Ethernet frame size of 64 octets. Thus, the Minimum UDP datagram size is set to 60, or equivalently, the minimum Ethernet frame size of 64 bytes minus 4 octets for the Frame Check Sequence (FCS).</p> <p>For IPv4 UDP packets, this means that any packet with a payload between 0 and N octets is not dropped when the default value is 60, where N is 18 that is, <math>(60 - 8(\text{UDP header length}) - 20(\text{IP header length}) - 14(\text{MAC header}))</math>. In the case of external VLANs, the MAC header is 18 octets, so N is 14.</p> <p>Set the value to a larger number when externally received IPv4 UDP packet payloads are expected to be at least 18 octets (or 14 for tagged VLAN traffic). For example, setting this value to 70 drops any IPv4 UDP Ethernet frames with a payload size of 0 to 27 octets (or 0 to 23 bytes for tagged VLAN traffic).</p> <p>For valid IPv6 UDP packets, the minimum Ethernet frame size is 66 octets, that is, <math>8(\text{UDP header length}) + 40(\text{IPv6 header length}) + 14(\text{MAC header length} + 4(\text{FCS}))</math> and the minimum UDP datagram ethernet frame size is 62 octets. For example, setting this value to 70 drops any IPv6 UDP Ethernet frames with a payload size of 0 to 7 octets (or 0 to 3 octets for tagged VLAN traffic).</p> |

| Parameter                    | Provisioning  |
|------------------------------|---|
| <b>Minimum Fragment Size</b> | Type the minimum size of an initial or intermediate fragment that is allowed.<br>The range varies from 60 to 1500.  |
| <b>Protocol Inspection</b>   | Select the Protocol inspection. The available options are None(0), SIP(1), and H248(2). The default value is None (0).<br><br>If SIP(1) is selected then SIP, STUN, SigComp is verified if the datagrams contain SIP, STUN or SigComp messages. The UDP datagram is dropped if it does not contain SIP, STUN, or SigComp message.<br><br>If H248(2) is selected then the message is dropped unless the UDP datagram contains H.248.<br><br>If the <b>Protocol Inspection</b> field is None(0), no UDP inspection is performed.<br><br><b>Note:</b> TCP packets are not inspected. |

For more information on the parameters, see the topic **Feph Flow Policy Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 5 Click **OK**.

**Result:** The Feph Flow Policy table attributes are provisioned successfully.

END OF STEPS

# Provision an Aggregate Packet Policy

## Purpose

This procedure provides the steps to provision an Aggregate Packet Policy.

## Before you begin

The pre-configured table attributes are auto-generated default values. It is recommended that the default values should not be increased. However, network requirements may suggest that these aggregate limits be decreased.

**Note:** For each externally received IP packet that matches a known flow, the FEPH determines whether that packet can be forwarded based on the aggregate packet policy for each of the following:

- The BEPH Aggregate Policy Group
- The FEPH Internal-facing Ethernet Port

If any of the aggregate packet policy statistics are at or above X% of their maximums, the packet is discarded.

- X = 100% if a Control Channel update for the associated Flow Table entry has been received at some time,
- X = 80% otherwise.

For each externally received IP packet for a new flow for which a BEPH Instance is chosen, the FEPH determines whether the packet or new flow would exceed the BEPH Aggregate Policy Group policies. If any of the aggregate packet policy statistics are at or above 80% of their maximums, the new flow is not accepted (and this packet is discarded). If any of the aggregate flow policy statistics are exceeded, the new flow is not accepted (and this packet is discarded).

For each externally received IP packet for a new flow for which a BEPH Instance is chosen, the FEPH determines whether the packet or new flow would exceed the Ethernet Port policies. If any of the aggregate packet policy statistics are at or above 80% of their maximums, the new flow is not accepted (and this packet is discarded).

Whenever a Flow Table main policy is installed, the FEPH marks/unmarks the flow as transient as follows:

- If the Flow Table entry timeout is set to  $\geq 600$  seconds, then the flow is marked as NOT transient.
- Else, the flow is marked as transient.

## Modifying the table attributes

Perform the following steps to modify the table attributes:

- 1 At the FS GUI main menu, select **IMS → FEPH Tables → Aggregate Packet Policy**.
- 2 Click the “+” symbol next to the **Aggregate Packet Policy** folder to expand this folder.
- 3 Right-click on the table and select **Open**.
- 4 Right-click the desired profile and select **Modify Table Attributes** .
- 5 Enter a brief description in the **Description** field.

**Note:** For all the following parameters, the value “**Drop all**” indicates that the FEPH will not forward any applicable packets, and a value of “**No limit**” indicates that the FEPH will not impose a rate limit.

- 6 The total number of physical bits (Ethernet header and payload) that are allowed to be forwarded through the entity per second is indicated in the **Total Bandwidth Limit (Mbits per sec)** field.
- 7 The total number of IP packets that are allowed to be forwarded through the entity per second is indicated in the **Total IP Packet Rate Limit (per sec)** field.  
A predetermined Transient flow aggregate packet rate limit (5%) is added to the existing provisioned aggregate packet rate limit .
- 8 The total number of initial packet fragments that are allowed to be forwarded through the entity per second is indicated in the **Total IP Packet Initial Fragment Rate Limit (per sec)** field.
- 9 The total number of ICMP messages that are allowed to be forwarded through the entity per second is indicated in the **Total ICMP Rate Limit (per sec)** drop-down list.

**10** Click **OK**.

E N D O F S T E P S

# Provision an Aggregate Flow Policy

## Purpose

This procedure provides the steps to provision an Aggregate Flow Policy.

## Before you begin

The pre-configured table attributes are auto-generated default values. It is recommended that the default values should not be increased. However, network requirements may suggest that these aggregate limits be decreased.

## Modifying the table attributes

Perform the following steps to modify the table attributes:

- 1 At the FS GUI main menu, select **IMS → FEPH Tables → Aggregate Flow Policy**.
- 2 Click the “+” symbol next to the **Aggregate Flow Policy** folder to expand this folder.
- 3 Right-click on the table and select **Open**.
- 4 Right-click the desired profile and select **Modify Table Attributes**.
- 5 Enter a brief description in the **Description** field.
- 6 The **Maximum Total Flows** field indicates the total number of flows that are allowed.
- 7 The **Maximum New Flow Rate (per sec)** field indicates the number of new flows that are allowed per second.
- 8 Click **OK**.

END OF STEPS

# Provisioning task flow for hardware acceleration

## Purpose

This topic describes the task flow that should be followed for provisioning the IPsec parameters.

### Setting the IPsec with FEPH Enabled IMS service

Before you begin to turn on or turn off the IPsec, ensure the following:

- IMS is FEPH Enabled
- P-CSCF SIPia ports on FEPH Enabled IMS use P-CSCF Profiles with no IPsec Secure Server Port specified.

### Turning on, or turning off the IPsec with FEPH Enabled IMS Service

Perform the following:

1. Change the Number of IPsec UEs of IMS to a zero value in the FEPH IPsec Parameters table
2. Change the IPsec Secure Server Port to zero in the P-CSCF profiles.

### Changing Number of IPsec UE value of the IMS

You can change the number of IPsec UE value in the following two situations:

1. If Number of IPsec UE(s) value is non-zero and it needs to change to zero, perform the following steps:
  - a. lock all the P-CSCFs on this FEPH Enabled IMS
  - b. disable the FEPH on the service
  - c. change the Number of IPsec UEs value to zero in the FEPH IPsec Parameters table.
2. If Number of IPsec UE(s) value is non-zero and it needs to change to another non-zero value, perform the following steps:
  - a. lock all the P-CSCFs on this FEPH Enabled IMS that have IPsec enabled (have a non-zero IPsec secure server port)
  - b. change the Number of IPsec UEs value to another non-zero value in the FEPH IPsec Parameters table

## IPsec parameters provisioning

1. In the P-CSCF profile, set the **Secure Server Port** field to enable IPsec support.

Ensure the following conditions:

- Support ESP Confidentiality can be checked only if Secure Server Port is entered
- Require ESP Confidentiality can be checked only if Support ESP Confidentiality is checked.
- IPSEC must be disabled (Secure Server Port must be zero) if Registration Suppression Enabled is set.
- If Access Type is DOCSIS, Remove P-Access-Network-Info must be Yes, Support TISPAN e2 Interface must be Disabled, Domain Name must be blank, and Secure Server Port for IPsec must be blank or zero.
- For the IPsec Secure Server port to be set, the new HWSecurity Software License must be installed.
- IPsec Secure Server Port can be specified (non-zero) only if the Security Gateway profile ID is specified and the Security Gateway profile ID has FEPH policies associated with it.
- If the IPsec Secure Server Port is set, the profile record can only be used by P-CSCF SIPia ports on IMS services that are on the SIP FEPH subnet. Check is needed in both the PCSCF profile (Modify) and SIPia port (Create and Modify).
- TLS Mandatory can be checked only if Support IPsec Capable UEs Only is unchecked.
- IPsec Secure Server port cannot be changed from zero to non-zero if any P-CSCF SIPia ports using the profile are associated with an FEPH Enabled IMS service and the Number of IPsec UEs value of the IMS is zero in the new FEPH IPsec Parameters table. The same check needs to be done for P-CSCF SIPia port insert/update of the Port Profile if the associated IPsec secure port is non-zero.
- A non-zero IPsec Secure Server port value cannot be specified if the value is already being used by any SIPia port (Port Number or TLS port number), or AGCF Gateway UDP/IP Port
- A IPsec Secure Server Port value cannot be modified from a non 0 value if any P-CSCF SIPia ports using the profile are unlocked (Administrative State = Unlocked). For example:
  - If the value needs to be changed from 6000 to zero, then all the P-CSCF SIPia ports using the profile must be locked (Administrative State = Locked).
  - If the value needs to be changed from 6000 to 6001, then all the P-CSCF SIPia ports using the profile must be locked (Administrative State = Locked).
- When changing from zero to a non-zero value, the P-CSCF SIPia ports need not be locked.

For example, if the value needs to be changed from zero to 6000, then the P-CSCF SIPia ports using the profile need not be locked.

- IPsec Secure Server Port values must be unique across different published realm's signaling v4 vlans (that is, signaling v4 vlan 800 and signaling v4 vlan 801 cannot be associated with the same IPsec Secure Server port value)

For provisioning the P-CSCF profile, see “[To activate PacketCable authentication in the P-CSCF profile](#)” (p. 4-104) and “[To provision IMS Signaling security](#)” (p. 4-108)

---

**2** Provision the IPsec parameter table

For provisioning information, see “[To provision an IPsec Parameters table](#)” (p. 5-155)

# Provision an Aggregate Policy Assignment

## Purpose

This procedure provides the steps to provision an Aggregate Policy Assignment.

## Before you begin

There is an automatically generated default assignment profile. The parameters within this assignment profile can be modified if required.

## Modifying the table attributes

Perform the following steps to modify the table attributes:

- 1 At the FS GUI main menu, select **IMS → FEPH Tables → Aggregate Policy Assignment**.
- 2 Click the “+” symbol next to the **Aggregate Policy Assignment** folder to expand this folder.
- 3 Right-click on the table and select **Open**.
- 4 Right-click the desired profile and select **Modify Table Attributes** .
- 5 Select the Aggregate Packet Policy ID to be enforced from the **Aggregate Packet Policy ID** drop-down list.
- 6 Select the Aggregate Flow Policy ID to be enforced from the **Aggregate Flow Policy ID** drop-down list.

**Note:** The **Aggregate Flow Policy ID** parameter is not applicable when the **Assignment Type** field is set to 'Internal Ethernet'.

- 7 Click **OK**.

END OF STEPS

# To provision an IPsec Parameters table

## Purpose

This procedure is used to provision an IPsec Parameters table.

## Description

The IPsec Parameters profile allows you to provision the total number of IPsec UEs supported, and the number of IPsec UEs supported for each individual FEPH candidate/enabled IMS service. This allows for IPsec UEs to be divided across the IMS Services. Even though the total number of IPsec UEs supported is 1,000,000, each IMS Service can have up to 548K IPsec connections, which is the maximum private IDs in a dedicated P-CSCF configuration.

**Note:** When provisioning the number of IPsec UEs supported for each IMS Service, ensure that the P-CSCF supports IPsec transport in that Service and the number of IPsec UEs does not exceed the expected number at those P-CSCF(s).

By default, one table for which one record is created during host\_manager startup when the FEPH service is detected. This record can be updated, or deleted. Deletion of this record is allowed only if the FEPH is no longer in the system.

If the number of IPsec UEs of a service instance has changed:

- If the old value is not equal to zero, all P-CSCFs on this service that use IPsec (have a profile with a non-zero Secure Port) must be locked (or the entire service can be locked). For example:
  - 1000 -> 0 (turning off)
  - 1000 -> 2000 (increasing)
  - 2000 -> 1000 (decreasing)

The P-CSCF need not be locked while updating from zero to X (turning on).

- If the new value is equal to zero, check if P-CSCFs with IPsec exists on this service and the service is FEPH enabled. If so, remove the IPsec secure port setting in the profile to produce an error.

### Note:

- The total number of IMS service IPsec UEs must be lesser than or equal to the total number of IPsec UEs supported on the FEPH.
- Whenever an IMS service node is deleted, the IPsec UE value of the service is reset to zero.

## Steps to provision a IPsec Parameter table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → FEPH Tables**.

**Result:** The **FEPH Tables** window is displayed.

- 2 In the left pane, expand the **IPsec Parameters** folder.

**Result:** The IPsec Parameters tables are listed under the folder in the left pane.

If the folder is empty, add a IPsec Parameter table.

Perform the following steps in the **FEPH Tables - IPsec Parameters** window to add, rename, or delete a IPsec Parameter table :

| If you want to ...               | then ...   |
|----------------------------------|--|
| add an IPsec Parameter table,    | <ol style="list-style-type: none"> <li>1 Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add IPsec Parameters table</b> window is displayed.</li> <li>2 From the <b>Table Number</b> list, select the table number.</li> <li>3 In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4 Click <b>OK</b>.</li> </ol> <i>End of steps</i> |
| rename an IPsec Parameter table, | <ol style="list-style-type: none"> <li>1 Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>Rename IPsec Parameters table</b> window is displayed.</li> <li>2 In the <b>Table Name</b> box, type a new table name.</li> <li>3 Click <b>OK</b>.</li> </ol> <i>End of steps</i>   |
| delete an IPsec Parameter table, | <ol style="list-style-type: none"> <li>1 Select the table, and then select <b>Tables → Delete table</b>.</li> <li>2 Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a IPsec Parameter table, ensure that no table entries are in use.</p> <i>End of steps.</i>   |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the IPsec Parameter table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 **Note:** The system does not allow adding attributes to the IPsec Parameters table.

Perform the following steps at the **FEPH Tables - IPsec Parameters** window to modify, or delete the IPsec Parameter table attributes:

| If you want to ...                          | then ...  |
|---|---|
| modify an IPsec Parameter table attributes, | <ol style="list-style-type: none"><li>1. In the right pane, select the profile that you want to modify.</li><li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>IPsec Parameters</b> window is displayed.</li><li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li></ol> <p><i>End of steps</i></p> |
| delete an IPsec Parameter table attributes, | <ol style="list-style-type: none"><li>1. In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li><li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li><li>3. Click <b>Yes</b> to confirm deletion.</li></ol> <p><i>End of steps.</i></p>                |

- 5 Provision the following parameters:

| Parameter                            | Provisioning  |
|--------------------------------------|---|
| <b>Total IPsec UEs Supported</b>     | Type the total number of IPsec UEs supported on the FEPH service  |
| <b>Available number of IPsec UEs</b> | This field displays the number of UEs available to be assigned across the individual services based off of the Total IPsec UEs Supported value. |

- 
- 6 To modify the service instance, select the service instance that you want to modify, and click **Modify**.

**Result:** The **Service instance IPsec UEs** window is displayed, where you can modify the values of the Service Instance and the Number of IPsec UEs.

For more information on the parameters, see the topic **IPsec Parameters** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

---

- 7 Click **OK**.

**Result:** The IPsec Parameter table attributes are provisioned successfully.

END OF STEPS

---

# Signaling Firewall configuration

## Overview

### Purpose

This section contains topics that describe the various aspects of Signaling Firewall, previously known as Secure External Access Lockout (SEAL), and the configuration procedures.

### Contents

|   |       |
|---|-------|
| External subnets                                      | 5-160 |
| Published NI IP addresses for FEPH and IMS services   | 5-161 |
| Default gateway and/or static routes for IMS services | 5-162 |

# External subnets

## Overview

This topic describes the external access subnet requirements for the FEPH service.

### External access subnets

The FEPH must have at least one external access subnet of type IPv4 or IPv6. If a second subnet is added, a maximum of two subnets are supported and these are designated “FEPH external access subnets”.

If two FEPH external access subnets are provisioned, then one must be of type IPv4 and the other must be of type IPv6. There cannot be two FEPH external subnets for one single type (IPv4 or IPv6).

# Published NI IP addresses for FEPH and IMS services

## Overview

This topic describes the published NI IP addresses for FEPH and IMS services.

### Published NI IP addresses

For a IMS service to be FEPH-enabled, the published NI IP addresses of the IMS service must be on the same subnet (the FEPH external access subnet) as the corresponding FEPH service published NI IP address.

### Example

If a single FEPH external access subnet is provided (IPv4 or IPv6), and the FEPH service has a published NI IP address on this subnet, then all FEPH-enabled IMS services must have the published NI IP addresses on that subnet.

If there are two FEPH external access subnets (one IPv4 and one IPv6), and the FEPH service has published NI IP addresses on both the subnets, then all FEPH-enabled IMS services must have their corresponding published NI IP address(es) (IPv4 and/or IPv6) on the corresponding FEPH external access subnet (IPv4 or IPv6).

# Default gateway and/or static routes for IMS services

## Overview

This topic describes the default gateway and/or static routes requirement for an IMS service to be FEPH-enabled.

## Default gateway and/or static routes

The IMS service must have either a default gateway or at least one static route that uses the FEPH external access subnet as its gateway. This ensures that appropriate outgoing packets are routed through the FEPH.

If a single FEPH external access subnet is provided (IPv4 or IPv6), and the FEPH Service has a published NI IP address on this subnet, then all FEPH-enabled IMS services must have a default gateway or at least one static route that uses this FEPH external access subnet as its gateway.

If there are two FEPH external access subnets (one IPv4 and one IPv6), and the FEPH service has published NI IP addresses on both the subnets, then all FEPH-enabled IMS services must have default gateways and/or static routes that use the FEPH external access subnets (Ipv4 and IPv6) as their gateway.

## Hosts with both FEPH-enabled and non-FEPH-enabled IMS services

If more than one IMS Service is present on a host, it is possible for some of the IMS services to be FEPH-enabled and others non-FEPH-enabled. To support this configuration, special care is needed in setting up static routes and default gateways.

The following alternative configurations are suggested:

1. Configure default gateways that specify the FEPH external access subnets as their gateway. Configure static routes (which will take precedence over the default gateways) for the non-FEPH-enabled IMS Services. In addition, for a FEPH-enabled IMS service, static routes must be defined for signaling (for example, DNS) that must not traverse the FEPH.
2. Configure default gateways that do not specify the FEPH external access subnets as their gateway. Configure static routes for the FEPH-enabled IMS Services that specify the FEPH external access subnets as their gateway.

# IMS Service Growth with an existing FEPH Service

## Overview

### Purpose

This section contains the topics that describe the IMS service growth and de-growth procedures with an existing FEPH service.

### Contents

|   |       |
|---|-------|
| To grow an IMS service that is FEPH-enabled               | 5-164 |
| To disable FEPH on an FEPH-enabled IMS service            | 5-166 |
| To add FEPH IPv4 or IPv6 capability for an IMS service    | 5-167 |
| To remove FEPH IPv4 or IPv6 capability for an IMS service | 5-170 |

# To grow an IMS service that is FEPH-enabled

## Purpose

Use this procedure to grow an IMS service that is FEPH-enabled (for IPv4 and/or IPv6). To FEPH-enable an IMS service that is not initially FEPH-enabled at all, it is necessary to de-grow the IMS service and then re-grow as described in this procedure.

## Procedure

Perform the following steps:

- 
- 1 If an IMS service is already present on the host to which the new IMS service is added, the host should be locked.

For the detailed procedures, refer “[To change the operational or administrative state of a SIPia port](#)” (p. 10-80).

**Note:** The steps 2 and 3 are applied only to grow an additional subnet (IPV4 or IPV6) when FEPH has only IPV6 or IPV4 subnet.

- 
- 2 If necessary, grow in a new FEPH external access subnet (IPv4 or IPv6).

For the detailed procedures, refer *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add a new external IPv4 subnet*

and *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add a new external IPv6 subnet*.

- 
- 3 **Note:** This step is not necessary if the FEPH service already has the required Published NI IP address assigned.

Add a new Published NI IP address (IPv4 or IPv6) using `ip_adm` on the FEPH external access subnet to the FEPH service.

For the detailed procedures, refer *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add a new external floating IPv4 address*

and *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add a new external floating IPv6 address*.

- 
- 4 Grow in the new IMS service. Follow the guidelines mentioned in “[Published NI IP addresses for FEPH and IMS services](#)” (p. 5-161) and “[Default gateway and/or static routes for IMS services](#)” (p. 5-162).

**Note:** The static routes must be added before the newly added IMS service is provisioned using the Provisioning GUI.

For the detailed growth procedures, refer topics *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, *Chapter 5: Manage system configuration - hardware growth > Growth implementation > To grow service of network boot hosts for multiple services* and *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, *Chapter 5: Manage system configuration - hardware growth > Growth implementation > To grow hardware and service of ATCA hosts*.

---

- 5 Verify that the IMS service is still shown with **FEPH Enabled = Yes** in the **System View** window of the Provisioning GUI windows for Configuration Management. See topic on *The System View window introduction* in Section *System View windows* in Chapter *Provisioning GUI windows for configuration management* from *Alcatel-Lucent 5400 Linux Control Platform User Interface*, 270-702-013 document for the **System View** window screen.

---

END OF STEPS

# To disable FEPH on an FEPH-enabled IMS service

## Purpose

Use this procedure to totally disable FEPH on an FEPH-enabled IMS service. The starting point for this procedure is an IMS service that is FEPH-enabled for IPv4, IPv6, or IPv4 and IPv6. The objective is that the resulting IMS service is not FEPH-enabled at all.

## Before you begin

Ensure that the IMS service is FEPH-enabled for IPv4, Ipv6, or IPv4 and IPv6.

## Procedure

Perform the following steps:

- 
- 1 The IMS service must be de-grown.

For the detailed procedures, refer topics *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, Chapter 6: *Manage system configuration - hardware de-growth > Degrowth implementation, topic: To de-grow service of multiple services on single processor* and *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter 6: *Manage system configuration - hardware de-growth > Degrowth implementation > To de-grow hardware and service of the hosts*.

- 
- 2 The IMS service must be re-grown with published NI IP address(es) that are NOT on the FEPH external access subnet.

For the detailed procedures, refer topics *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, Chapter 5: *Manage system configuration - hardware growth > Growth implementation > To grow hardware and service of ATCA hosts* and *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, Chapter 5: *Manage system configuration - hardware growth > Growth implementation > To grow service of network boot hosts for multiple services*.

---

END OF STEPS

# To add FEPH IPv4 or IPv6 capability for an IMS service

## Purpose

Use this procedure to add FEPH capability for an IMS service for the following scenarios:

- FEPH IPv6 capability when FEPH IPv4 capability is previously added
- FEPH IPv4 capability when FEPH IPv6 capability is previously added

## Procedure

Perform the following steps:

- 
- 1 Lock the IMS service and remove all the SIPia ports associated to this IMS service.

For the detailed procedures, refer “[To change the operational or administrative state of a SIPia port](#)” (p. 10-80) and “[To provision a SIPia port](#)” (p. 10-40).

---

- 2 Delete the IMS service using the Provisioning GUI. This action makes the Host Duplex-Failed.

For the detailed procedures, refer “[To provision an IMS Service association](#)” (p. 10-20).

---

- 3 If necessary, grow in a new FEPH external access subnet (IPv4 or IPv6).

For the detailed procedures, refer *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add a new external IPv4 subnet*

and *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add a new external IPv6 subnet*.

---

- 4 **Note:** This step is not necessary if the FEPH service already has the required Published NI IP address assigned.

Add a new IPv4 or IPv6 Published NI IP address (using ip\_adm) on the FEPH external access subnet to the FEPH service.

The addition of an IP address to the FEPH service depends on whether the required IP address is available on the FEPH external access subnet.

For the detailed procedures, refer *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add a new external floating IPv4 address* and *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add a new external floating IPv6 address*.

- 
- 5 Add a new IPv4 or IPv6 Published NI IP address (using ip\_adm) on the FEPH external access subnet to the IMS service.

The addition of an IP address to the IMS service depends on whether the required IP address is available on the FEPH external access subnet.

For the detailed procedures, refer *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add a new external floating IPv4 address* and *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add a new external floating IPv6 address*.

- 
- 6 Add Static Routes to the IMS Service using the FEPH external access subnet (IPv4 or IPv6) and/or modify the Default Gateway for the IMS Service to use the new FEPH external access subnet (IPv4 or IPv6) using MI GUI. Please see “[Default gateway and/or static routes for IMS services](#)” (p. 5-162).

For the detailed procedures, refer *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add or delete static routes for a service* and *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To modify the Default Gateway data for a service*.

- 
- 7 Complete IMS service provisioning and bring IMS service into service.

For the detailed procedures, refer “[IP Session Control configuration flow](#)” (p. 1-5).

- 
- 8 Check the **FEPH Enabled Services** table in FEPH Tables to verify the FEPH-Enabled status of an IMS Service. See the topic, “The IMS FEPH Tables menu” in the ISC Application User Guide.

END OF STEPS

---

# To remove FEPH IPv4 or IPv6 capability for an IMS service

## Purpose

Use this procedure to remove FEPH IPv4 or IPv6 capability from an IMS service.

**Note:** FEPH should be previously enabled for IPv4 and IPv6.

## Procedure

Perform the following steps:

- 1 Login to the MI as *root* and navigate to **Management Interface** → **Office** → **Configuration Management** → **Network Interface**.
- 2 Point to the IMS group in the service instances and right-click on it.  
**Result:** A pop-up window appears listing the tasks that are allowed.  
Select *Lock Service Instance* from the list of tasks to lock the IMS service.
- 3 Remove IPv4 or IPv6 static routes that specify the FEPH external access subnet (IPv4 or IPv6).  
For the detailed procedure, refer *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add or delete static routes for a service*.
- 4 If necessary, modify the Default Gateway that specifies the FEPH external access subnet (IPv4 or IPv6).  
For the detailed procedure, refer *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To modify the Default Gateway data for a service*.
- 5 Remove the IPv4 or IPv6 IP address assigned from the Published NI for the IMS service (that is, set to None using MI GUI).

For detailed procedure, refer *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To modify the IP addresses of a Network Interface*.

---

**6** Change status of the IMS service to Duplex-Failed.

For detailed procedure, refer *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, Chapter 4: *Manage system configuration - View or control the operational state* > *View or control the operational state* > *To modify the state of a network boot host*.

---

**7** Restore the IMS service pair to active or standby state.

---

**8** Verify that the IMS service is still shown with **FEPH Enabled = Yes** in the **System View** window of the Provisioning GUI windows for Configuration Management. Please see topic on *The System View window introduction* in Section *System View windows* in Chapter *Provisioning GUI windows for configuration management* from *Alcatel-Lucent 5400 Linux Control Platform User Interface*, 270-702-013 document for the **System View** window screen.

---

**9** Login to the MI as *root* and navigate to **Management Interface** → **Office** → **Configuration Management** → **Network Interface**.

---

**10** Point to the IMS group in the service instances and right-click on it.

**Result:** A pop-up window appears listing the tasks that are allowed.

Select *Unlock Service Instance* from the list of tasks to unlock the IMS service.

END OF STEPS

---

# Signaling Firewall Service Growth with existing IMS Services

## Overview

### Purpose

This section contains the topics that describe the FEPH service growth and de-growth procedures with existing IMS services.

### Contents

|  |       |
|--|-------|
| Signaling Firewall growth preparation and planning           | 5-173 |
| To grow Signaling Firewall and FEPH on an existing network   | 5-179 |
| To grow Signaling Firewall and FEPH on a new network         | 5-191 |
| FEPH growth cleanup  | 5-200 |
| Service growth of FEPH service on HSPP4 of Malban (Hub) card | 5-201 |
| fehpGrowth command   | 5-208 |
| FEPH growth error-handling                                   | 5-211 |
| FEPH growth worksheet  | 5-212 |

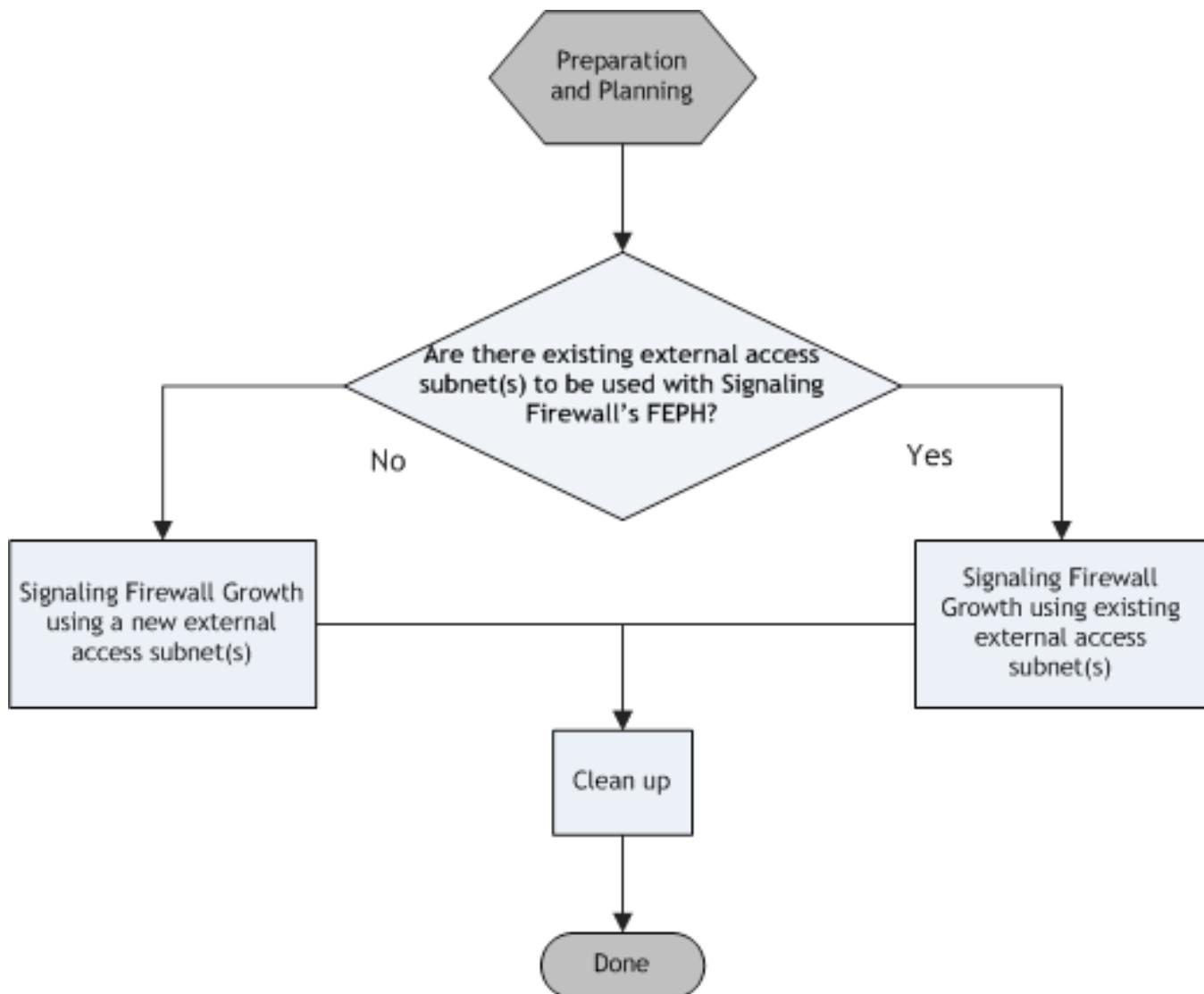
# Signaling Firewall growth preparation and planning

## Overview

Use this procedure for Signaling Firewall growth preparation and planning before you proceed to any of the following Signaling Firewall growth scenarios:

- “To grow Signaling Firewall and FEPH on an existing network” (p. 5-179)
- “To grow Signaling Firewall and FEPH on a new network” (p. 5-191)

The following figure provides a view of the overall Signaling Firewall growth process.



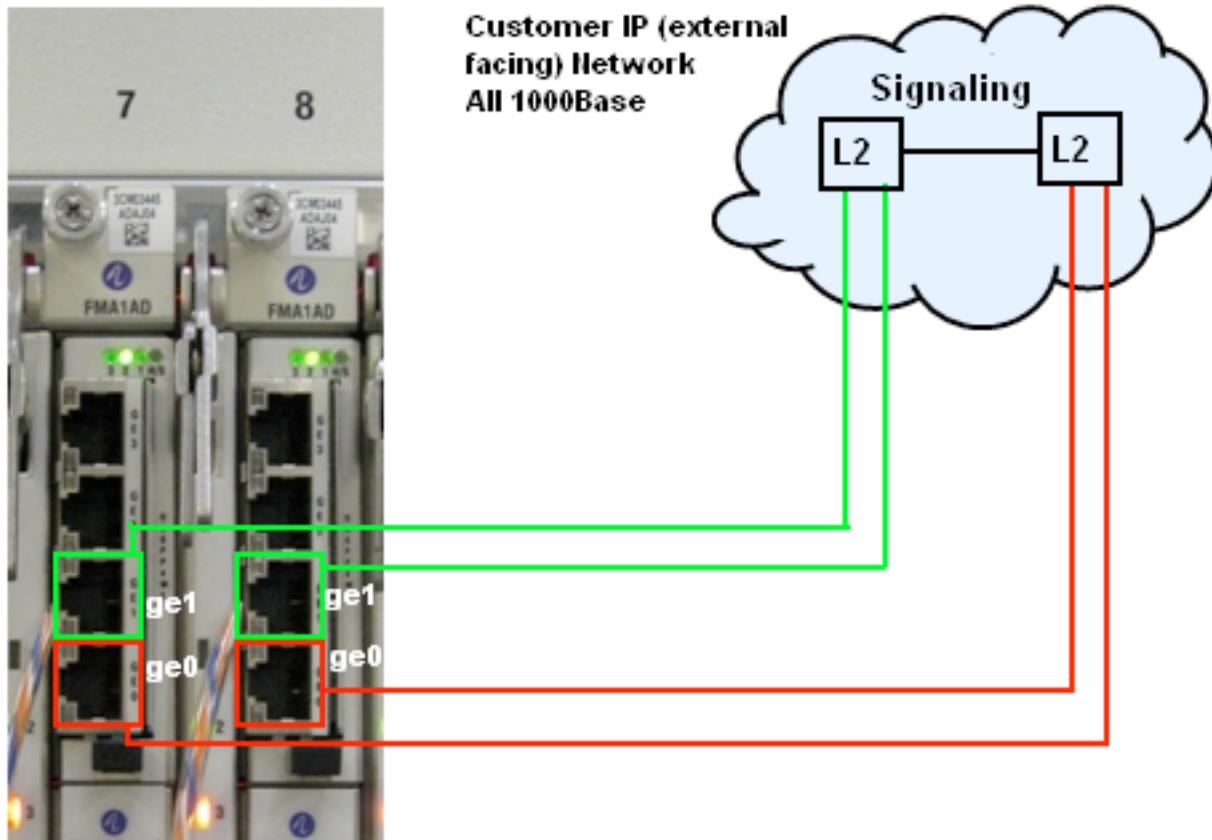
## Procedure

Perform the following :

- 1 Verify the availability of *Microsoft Excel*.

*Microsoft Excel* is used to view or edit the Signaling Firewall growth worksheet.

- 2 Ensure that a pair of FMA1AD cards and a 1G cross connect cable are available. See *Alcatel-Lucent 5400 Linux control platform Configuration management*, 270-702-014, Chapter: *Platform hardware conversion*, Topic: *To convert hub without HSPP4 to hub with HSPP4 - Step 34*.
- 3 Ensure four cables are available to connect from the two HSPP4 front panels to the customer network.



The four connections are required for the following reasons:

- A pair of HSPP4 cards host the FEPH (Front-End Packet Handler) service that provides a SIP Firewall defense for the untrusted access subnet traffic destined to the P-CSCFs.
- The FEPH service runs in active or standby mode; so at any given time only one of the FEPHs is active and handling live access traffic.
- At any given time, there is only one active Ethernet port out of the pair of HSPP4 ports on the active FEPH HSPP4. Neither of the Ethernet ports on the standby FEPH HSPP4 carry any access traffic.
- All of the IPs in the access subnet are advertised only on the active Ethernet port of the active FEPH.

In Signaling Firewall configuration:

- An IMS service with P-CSCFs has an access IP address.
  - There is one access IP for the FEPH pair.
  - Only the access IPs for the IMS services are used for access traffic.
  - The FEPH access IP is required for implementation. It does not receive any traffic.
  - The IP addresses are floating IP addresses and “Owned” by the active FEPH or HSPP4.
- Various redundancy scenarios are supported.

Listed below are a few examples:

- If the Cable (or Router/Switch) connected to the active Ethernet cable on the active FEPH HSPP4 card fails, traffic is switched to the other Ethernet port on the active FEPH.

For example, in the figure “Procedure” (p. 5-174), the ge0 port (in red color) on active card 7 fails, traffic is switched to port ge1 in green on the same card.

- If the HSPP4 experiences a hardware failure, the active FEPH service switches to the HSPP4 on the other Malban card.

For example, in the figure “Procedure” (p. 5-174), if both ge0 and ge1 ports on card 7 fail, the ports ge0 and ge1 on card 8 becomes active and carries the packet traffic.

- When the system runs Simplex as part of maintenance scenarios such as Software Update, the active FEPH completely retains the redundant communication.

Advantages of having four connections are listed below:

- Full Ethernet redundancy is maintained in addition to the blade or software redundancy.
- Untrusted access traffic is separated from trusted core or OAM traffic.

For example, untrusted traffic cannot starve out trusted traffic. The trusted traffic never faces competition for bandwidth on the link.

- 
- 4** Ensure adequate Ethernet ports are present to accommodate new connections to the customer network. As a part of migration using Signaling Firewall, four new Ethernet connections must be added between the 5450 ISC and Layer 2 equipment of the service provider. Two connections terminate on the faceplate of each of the HSPP4 AMC cards on the 5450 ISC. Other two connections terminate on each of the two Layer 2 devices on the external equipment.

During service migration for the existing network with IMS services growth case, the 5450 ISC does not give explicit requirements on how to deliver packets to the current Malban interface and support seamless transition to the HSPP4 front panel interface without causing disruption to the current Malban interface.

**Note:** This implementation is left up to the discretion of the network engineer, but must be completed before attempting the in-service migration.

For example: The ethernet ports connected to the current Malban interface and the ethernet ports connected to the new HSPP4 front panel interface have to be placed in the same VLAN.

---

- 5** Login to an active MI host as *root* and execute the following command:

**fephGrowth -m**

The following list is generated:

- Identification of all existing IMS services and SIPia ports configured in the office. This includes the external floating IP addresses being used to service UE SIP traffic.
- Configuration gaps for each IMS service on which FEPH has to be enabled. These gaps have to be fixed prior to enabling FEPH on the IMS service.

The possible configuration gaps are listed below:

- The missing software license for FEPH and Integrated Security Gateway must be provided. The software licensing key values for FEPH and the security gateway are **FEPH** and **iSGW-A** respectively. The missing software license prohibits assigning FEPH flow polices to iSGW profiles.
- Published NI IP addresses (IPv4 and/or IPv6) are required on the IMS service.

If the IMS service that is to be FEPH enabled does not have a published NI, then new external floating IP addresses must be added to that IMS service.

For detailed procedures on how to add new external floating IP addresses (IPv4 or IPv6), see, *Alcatel-Lucent 5400 Linux Control Platform Configuration Management*, 270-702-014 Chapter: *Manage system configuration - IP configuration*, Section: *IP address and route configuration*, Topics: *To add a new external floating IPv4 address and To add a new external floating IPv6 address*.

**Note:** It is not recommended that a new Published NI be added to an IMS Service that already hosts P-CSCF SIPia ports.

- Ensure the parameter **Enable 2 NIs for SIP** on all P-CSCF SIPia ports on the IMS service is set.
- Remove IBCF SIPia ports if any from the IMS service.
- Add a **Security Gateway Profile ID** reference on the **Security Parameters** tab of applicable P-CSCF Profile entries used on the IMS service.

This operation is potentially service-impacting if the iSGW rate limits are such that they limit incoming SIP message traffic.

- Set the value of secure ports in the **IPSec Parameters** option on the **Security Parameters** tab of applicable P-CSCF Profile entries used in the IMS service to zero.
- Identification of all existing static routes and default gateways for each configured IMS, FS5K, and H248 service.
- Identification of all existing external subnets in the office.

**Note:** The command **fephGrowth -m** also performs a thorough check of the system status. Ensure that all problems identified as a result of the check are fixed before you proceed further.

For a sample output, see [Appendix A, “ Sample output for fephGrowth -m”](#).

---

## 6 Select the external subnets to be used as FEPH external access subnets.

This selection determines the following:

- If one or more new subnets have to be added to serve as FEPH external access subnets or if the existing external access subnets are reused.
- The Signaling Firewall growth procedures to be followed.
  - For Signaling Firewall and FEPH growth on an existing network, see [“To grow Signaling Firewall and FEPH on an existing network” \(p. 5-179\)](#)
  - OR
  - For Signaling Firewall and FEPH growth on a new network, see [“To grow Signaling Firewall and FEPH on a new network” \(p. 5-191\)](#)

- 
- 7 The IMS services to be FEPH-enabled are selected based on the type of growth. The two types of growth scenarios are:
1. A migration of existing IMS services to become FEPH-enabled or Signaling Firewall protected, that is, growing FEPH on an existing network. In this growth scenario, the user can exclude an IMS service which would be converted or include an IMS service.
  2. Migration where each IMS service is moved, that is, growing FEPH on a new network. Here the IMS services to be “FEPH-enabled” are identified.

Before you begin with the growth procedures, perform the following:

- During Signaling Firewall growth, FEPH-related data is included in the P-CSCF profile. If a P-CSCF profile is shared between two IMS services and if only one of the IMS services are selected for growth procedures, unshare the P-CSCF profiles.

This specific remedial step is not a part of the Signaling Firewall growth procedure.

After performing the above-mentioned action, re-execute the command

**fephGrowth -m**.

---

END OF STEPS

---

# To grow Signaling Firewall and FEPH on an existing network

## Purpose

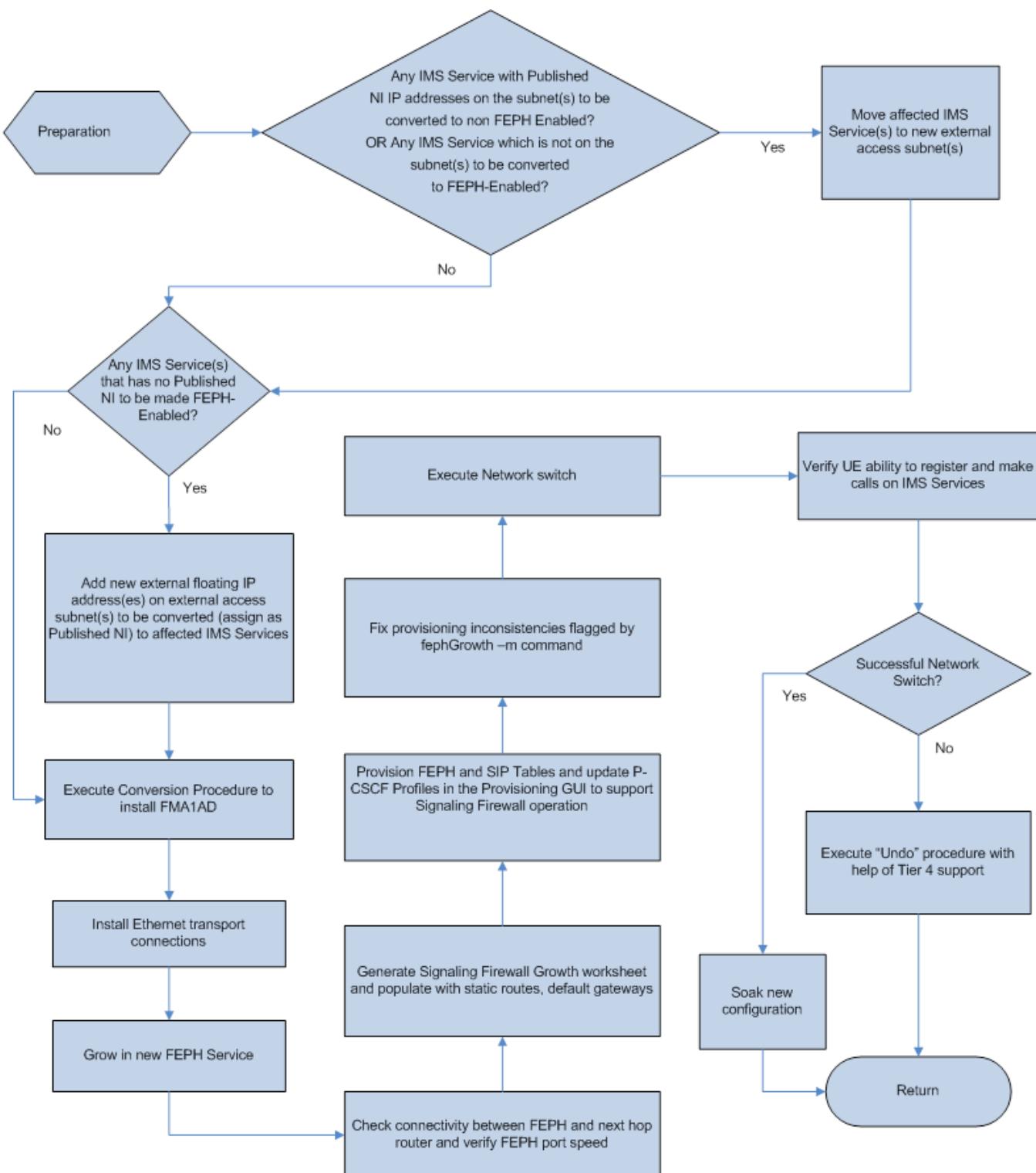
This topic describes the procedure to grow Signaling Firewall and FEPH on an existing network.

## Before you begin

**Note:** Ensure that the following procedure has been executed “[Signaling Firewall growth preparation and planning](#)” (p. 5-173).

**Note:** For information on error-handling during Signaling Firewall growth procedures, see:“[FEPH growth error-handling](#)” (p. 5-211)

The following figure shows the flow of the Signaling Firewall growth operation using existing external access subnets:



## Procedure

Perform the following steps:

---

### 1 Preparation

Following are the preparation steps to grow Signaling Firewall and FEPH on to existing networks:

- Ensure the intended FEPH external subnets have only FEPH service or IMS service Published NI IP addresses owned by the 5400 Linux CP and all IP addresses on the subnet are owned by the 5400 Linux CP.
- This verification can be performed by the following methods:
- Procedural: Perform a verification of all IP addresses on the subnets owned by the 5400 Linux CP. This is done by inspecting the network plan of the office.
  - Automated: Search the 5400 Linux CP subnet IP addresses in the SCDT data and verify if they are assigned only to the Published NI for the FEPH and IMS services. This is a verification step that is performed at the beginning of the execution of the following commands: `fephGrowth -s` and `fephGrowth -g`.

- Ensure adequate IP address space exists in the subnets to accommodate addition of FEPH IP addresses. Select the IP addresses to be assigned to the FEPH service.
- Review the selection of IMS services to be FEPH-enabled. This is an “automatic” selection based on the existing assignment of Published NI IP addresses to IMS services.
- For each IMS service on which FEPH has to be enabled, plan new static route and default gateway configuration. The new static route ensures that only the desired signaling traffic is routed through FEPH and prevents other signaling traffic (for example, DNS, diameter traffic, and so on) from going through the FEPH.

If the default gateway on a host is configured such that it directs traffic through the FEPH, static routes need to be planned or provided to prevent non-UE signaling traffic (for example, DNS, Diameter traffic) and H.248 and FS5K Service signaling traffic from traversing the FEPH.

FEPH and Signaling Firewall are SIP enabled Firewall. It does not allow any other traffic or protocols to pass through. Hence there is a need to ensure that both the trusted and untrusted traffic are properly identified. A static route has to be added for the trusted traffic to go through the FEPH. All the traffic with the NI Type published goes through the FEPH.

---

### 2 Move the affected IMS services to new external access subnets

**Note:** This step is not mandatory and should be executed only when necessary. For most Signaling Firewall growth operations, this step is not necessary. When the IMS services are moved to a different network, it is service impacting.

During Signaling Firewall growth operation, the packet path for an external access subnet is switched. The packet path now goes through an Ethernet uplink on Malban and is switched to an Ethernet uplink on the HSPP4. Some IMS services may have Published NI IP addresses on the subnets to be switched. If there are IMS Services on the subnets to be switched (henceforth referred to as "affected IMS Services") that the user does not want to be made FEPH-Enabled, then those IMS Services should be moved to a different external access subnets prior to the Signaling Firewall growth operation.

If this Signaling Firewall growth procedure is used to FEPH-enable an IMS service that is not yet on the external access subnets that are to be switched, the Published NI IP address for the IMS services must be moved to the external access subnet that is to be switched.

To move IMS services to new external access subnets, perform the following steps:

- Add new external access subnets (IPv4 or IPv6), if required. For detailed procedures see:

*Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014 , Chapter: Manage system configuration - IP configuration, Section: IP address and route configuration, Topics: To add a new external IPv4 subnet and To add a new external IPv6 subnet*

- Add new external floating IP addresses (IPv4 or IPv6) as "Unassigned" NI for the IMS services on the new subnets. For detailed procedures see:

*Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014, Chapter: Manage system configuration - IP configuration, Section: IP address and route configuration, Topics: To add a new external floating IPv4 address and To add a new external floating IPv6 address.*

- Change the Published NI IP address on the "affected" IMS services to the newly added external floating IP addresses. For detailed procedure, see:

*Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014, Chapter: Manage system configuration - IP configuration, Section: IP address and route configuration, Topic: To modify the IP addresses of a Network Interface.*

- Switch over the affected IMS services. For detailed procedure, see:

*Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014, Chapter: Manage system configuration - view or control the operational state, >View or control the operational state, > To modify the state of a network boot host.*

**Note:** If a P-CSCF SIPia port on one of the affected IMS services shares a P-CSCF profile with SIPia ports residing on an IMS service that is to be made FEPH-enabled, unshare the P-CSCF profile on that SIPia port.

---

### 3 Add new Published NI IP addresses to IMS services

If an IMS service to be made FEPH-enabled does not have Published NI IP addresses, then add new external floating (IPv4 or IPv6) IP addresses (assigned to the Published NI) to the IMS service.

See:

*Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014, Chapter: Manage system configuration - IP configuration, Section: IP address and route configuration, Topics: To add a new external floating IPv4 address and To add a new external floating IPv6 address.*

**Note:** It is recommended that a new Published NI IP address is not added to an IMS service that already hosts P-CSCF SIPia ports.

---

### 4 Execute the conversion procedure to install FMA1AD

For information on the conversion procedure, see, *Alcatel-Lucent 5400 Linux Control Platform Configuration Guide, 270-702-014 Chapter 7Platform hardware conversion section Platform hardware conversion.*

---

### 5 Install Ethernet transport connections

To install Ethernet transport connections between HSPP4 face plate and the external network equipment, see *Alcatel-Lucent 5400 Linux Control Platform Configuration Guide, 270-702-014 Chapter 5Manage system configuration – hardware growth section Growth system preparation.*

---

### 6 Grow in the new FEPH service

To grow FEPH service on HSPP4 of Malban (Hub) card, see: “[Service growth of FEPH service on HSPP4 of Malban \(Hub\) card](#)” (p. 5-201)

**Note:** Assign the NI type “Unassigned” for the FEPH IP addresses. Hit the “Return” key when prompted for the NI type for FEPH. During the growth scenario, the command **fephGrowth -s** is used to change the NI type of FEPH addresses to “Published”.

As the FEPH NI type is “Unassigned” and the external access subnets do not use the HSPP4 ports, the FEPH service initially comes up in a degraded state. This is resolved on execution of the command **fephGrowth -s**.

**Note:** When the FEPH service comes up with a degraded status, do not execute the command **fephGrowth -m** until this command is executed in [Step 11](#) of the Signaling Firewall growth procedure.

**Example:** The following error occurs if the command **fephGrowth -m** is executed before [Step 11](#)

```
> ./fephGrowth -m
fephGrowth: started 08/05/10 10:17
Verifying config host (10.82.194.0) is reachable
config host (10.82.194.0) ping test completed successfully
fephGrowth.ksh Process mapoffice request
Running su_health -a ...
*****Warning: There are errors after running su_health -
a*****
ERROR: chk_new_connectivity: Connectivity check for card cpr02-
s00c07h4
failed.
ERROR: chk_new_connectivity: Connectivity check for card cpr02-
s00c08h4
failed.
ERROR: chk_new_connectivity: Failed with 2 errors
ERROR: chk_new_connectivity FAILED.
ERROR: chk_all: Completed with ERRORS.
ERROR: chk_all: Completed with ERRORS.
ERROR: chk_all failed.
```

## 7 Check connectivity between FEPH and the next hop router. Verify the FEPH port speeds.

Ensure that the connectivity between the FEPH and the next hop router is properly established.

Check the following:

- Ensure proper physical connections to the next hop router.
- Ensure proper configuration of FEPH service and next hop router.

The command **fephGrowth -c** is provided to verify proper communication.

**Note:** Before proceeding with the subsequent growth steps:

- Ensure that a successful result is obtained from execution of the command **fephGrowth -c**.
- Verify the connection speed output. The maximum speed is 1Gigabit. The speed may be lower depending on the L2 router that the FEPH is connected to.

The current connection speeds are displayed near the end of the **fephGrowth -c** output.

- Ensure the FEPH service is back in an active or standby configuration. This operation may take 10 min.

**Example:** Below is a sample output obtained on execution of the command

**fephGrowth -c:**

```
> ./fephGrowth -c
fephGrowth: started 08/09/10 14:15
Verifying config host (10.82.194.0) is reachable
config host (10.82.194.0) ping test completed successfully
fephGrowth Process conncheck request
=====Checking the connectivity for
IPv4=====
Dharma/isql Version 09.00.0000
Dharma Systems Inc (C) 1988-2003.
Dharma Systems Pvt Ltd (C) 1988-2003.
ucl force OOS succeeded poolType 40, poolID 0, poolMember 0
ucl force OOS succeeded poolType 40, poolID 0, poolMember 1
Checking the connection for feph cpr02-s00c07h4
Verifying feph host (cpr02-s00c07h4) is reachable
feph host (cpr02-s00c07h4) ping test completed successfully
Stop aim for feph host ( cpr02-s00c07h4 ) ..... done!
rmmod kfeph for feph host ( cpr02-s00c07h4 ) ..... done!
Add the base to cpr02-s00c07h4 via ipm_cli ..... done!
Add FEPH access ip ( 135.1.184.33 ) to cpr02-s00c07h4 via ipm_cli
..... done!
Add default gateway ip ( 135.1.184.62 ) to cpr02-s00c07h4 via ipm_
cli ..... done!
Add the ARP ip ( 135.1.184.62 ) to cpr02-s00c07h4 via ipm_cli .....
done!
Verifying ims host (cpr02-s00c13h0) is reachable
ims host (cpr02-s00c13h0) ping test completed successfully
Verifying feph host (cpr02-s00c07h4) is reachable from ims host (
cpr02-s00c13h0 )
feph host (cpr02-s00c07h4) ping test from ims host (cpr02-s00c13h0)
completed successfully
traceroute to 135.1.184.33 (135.1.184.33), 6 hops max, 40 byte
packets
1 135.1.184.33 (135.1.184.33) 0.226 ms 0.307 ms 0.223 ms
The connection check for feph host (cpr02-s00c07h4) is success!
Checking the connection for feph cpr02-s00c08h4
Verifying feph host (cpr02-s00c08h4) is reachable
feph host (cpr02-s00c08h4) ping test completed successfully
Stop aim for feph host ( cpr02-s00c08h4 ) ..... done!
rmmod kfeph for feph host ( cpr02-s00c08h4 ) ..... done!
Add the base to cpr02-s00c08h4 via ipm_cli ..... done!
Add FEPH access ip ( 135.1.184.33 ) to cpr02-s00c08h4 via ipm_cli
..... done!
```

```

Add default gateway ip ( 135.1.184.62 ) to cpr02-s00c08h4 via ipm_
cli ..... done!
Add the ARP ip ( 135.1.184.62 ) to cpr02-s00c08h4 via ipm_cli .....
done!
Verifying ims host (cpr02-s00c13h0) is reachable
ims host (cpr02-s00c13h0) ping test completed successfully
Verifying feph host (cpr02-s00c08h4) is reachable from ims host (
cpr02-s00c13h0 )
feph host (cpr02-s00c08h4) ping test from ims host (cpr02-s00c13h0)
completed successfully
traceroute to 135.1.184.33 (135.1.184.33), 6 hops max, 40 byte
packets
1 135.1.184.33 (135.1.184.33) 0.235 ms 0.294 ms 0.226 ms
The connection check for feph host (cpr02-s00c08h4) is success!
=====Checking the connectivity for
IPv6=====
Dharma/isql Version 09.00.0000
Dharma Systems Inc (C) 1988-2003.
Dharma Systems Pvt Ltd (C) 1988-2003.
ucl force OOS succeeded poolType 40, poolID 0, poolMember 0
ucl force OOS succeeded poolType 40, poolID 0, poolMember 1
Checking the connection for feph cpr02-s00c07h4
Verifying feph host (cpr02-s00c07h4) is reachable
feph host (cpr02-s00c07h4) ping test completed successfully
Stop aim for feph host ( cpr02-s00c07h4 ) ..... done!
rmmod kfeph for feph host ( cpr02-s00c07h4 )..... done!
Add the base to cpr02-s00c07h4 via ipm_cli ..... done!
Add FEPH access ip ( 2802:5450:0001:ca25:0000:0000:0000:0001 ) to
cpr02-s00c07h4 via ipm_cli ..... done!
Add default gateway ip ( 2802:5450:1:ca25:ffff:ffff:ffff:fffe ) to
cpr02-s00c07h4 via ipm_cli ..... done!
Add the ARP ip ( 2802:5450:1:ca25:ffff:ffff:ffff:fffe ) to cpr02-
s00c07h4 via ipm_cli ..... done!
Verifying ims host (cpr02-s00c13h0) is reachable
ims host (cpr02-s00c13h0) ping test completed successfully
Verifying feph host (cpr02-s00c07h4) is reachable from ims host (
cpr02-s00c13h0 )
feph host (cpr02-s00c07h4) ping test from ims host (cpr02-s00c13h0)
completed successfully
traceroute to 2802:5450:0001:ca25:0000:0000:0000:0001 (2802:5450:1:
ca25::1), 6 hops max, 40 byte
packets
1 2802:5450:1:ca25::1 (2802:5450:1:ca25::1) 0.313 ms 0.282 ms 0.133
ms
The connection check for feph host (cpr02-s00c07h4) is success!
Checking the connection for feph cpr02-s00c08h4
Verifying feph host (cpr02-s00c08h4) is reachable
feph host (cpr02-s00c08h4) ping test completed successfully
Stop aim for feph host ( cpr02-s00c08h4 ) ..... done!
rmmod kfeph for feph host ( cpr02-s00c08h4 )..... done!
Add the base to cpr02-s00c08h4 via ipm_cli ..... done!

```

```

Add FEPH access ip ( 2802:5450:0001:ca25:0000:0000:0000:0001 ) to
cpr02-s00c08h4 via ipm_cli ..... done!
Add default gateway ip ( 2802:5450:1:ca25:ffff:ffff:ffff:ffff ) to
cpr02-s00c08h4 via ipm_cli ..... done!
Add the ARP ip ( 2802:5450:1:ca25:ffff:ffff:ffff:ffff ) to cpr02-
s00c08h4 via ipm_cli ..... done!
Verifying ims host (cpr02-s00c13h0) is reachable
ims host (cpr02-s00c13h0) ping test completed successfully
Verifying feph host (cpr02-s00c08h4) is reachable from ims host (
cpr02-s00c13h0 )
feph host (cpr02-s00c08h4) ping test from ims host (cpr02-s00c13h0)
completed successfully
traceroute to 2802:5450:0001:ca25:0000:0000:0000:0001 (2802:5450:1:
ca25::1), 6 hops max, 40 byte
packets
1 2802:5450:1:ca25::1 (2802:5450:1:ca25::1) 0.285 ms 0.245 ms 0.117
ms
The connection check for feph host (cpr02-s00c08h4) is success!
=====Initialize the feph
host=====
restore succeeded poolType 40, poolID 0, poolMember 0
restore succeeded poolType 40, poolID 0, poolMember 1
s00c07h4 is being initialized
s00c08h4 is being initialized
host = cpr02-s00c07h4, ipd_port = 0, Name = eth2 (up), PortType =
external, PortSpeedInst =
1000000000
host = cpr02-s00c07h4, ipd_port = 1, Name = eth3 (up), PortType =
external, PortSpeedInst =
1000000000
host = cpr02-s00c08h4, ipd_port = 0, Name = eth2 (up), PortType =
external, PortSpeedInst =
1000000000
host = cpr02-s00c08h4, ipd_port = 1, Name = eth3 (up), PortType =
external, PortSpeedInst =
1000000000
fephGrowth: Completed Successfully.
fephGrowth ended 08/09/10 14:1

```

## 8 Populate the worksheet with static routes, default gateways, and NI changes

The user must begin looking at the worksheet and the network immediately. There is some delay between replacing the HUB with an FMA1AD version and doing the subsequent “worksheet” step.

To populate the worksheet with static routes, default gateways, and NI changes, see:  
[“FEPH growth worksheet” \(p. 5-212\)](#)

## 9 Provision the FEPH Tables , SIP Tables and update the P-CSCF Profile Entries.

- Populate the FEPH Tables data (IMS → FEPH Tables) with FEPH Flow and Aggregate Policy information. This must be done after the FEPH Service is grown. The FEPH Service growth step results in the automatic creation of FEPH default data.

For more information on how to provision the FEPH tables, see: “[Provision the Signaling Firewall](#)” (p. 1-62)

**Note:** Perform the provisioning of the FEPH tables after the FEPH service is grown. The FEPH service growth results in the automatic creation of FEPH default data except the Trusted Default policy in the Flow Policy. The user is required to create the Trusted Default policy.

- Add iSGW policy and profile entries in the SIP tables (IMS → SIP Tables). This includes SIP Flow and Aggregate Trusted Rate Limit Rule Sets, SIP Flow and Aggregate Untrusted Rate Limit Rule Sets, Flow and Aggregate Source Address Policy entries and Security Gateway Profile entries. This includes populating the FEPH Policies section of the applicable Security Gateway Profile entries. Modify the existing P-CSCF profiles used on intended FEPH-Enabled IMS Services so that they reference the appropriate Security Gateway Profile entries.

For detailed provisioning procedures see:

- “[To provision an SIP Aggregate Trusted/Untrusted Rate Limit Rule Set](#)” (p. 5-72)
- “[To provision an SIP Flow Trusted/Untrusted Rate Limit Rule Set](#)” (p. 5-68)
- “[To provision an Aggregate Source Address Policy](#)” (p. 5-80)
- “[To provision a Flow Source Address Policy](#)” (p. 5-76)
- “[To provision a Security Gateway Profile](#)” (p. 5-90)

Include Integrated Security Gateway policy and profile entries in the SIP tables (IMS → SIP Tables). Finally

To populate the FEPH Policies section of the applicable Security Gateway Profile entries, see: “[Provision Integrated Security Gateway \(iSGW\)](#)” (p. 1-51)

To modify the P-CSCF profiles of the FEPH-enabled IMS services, see: “[To provision PCSCF profile](#)” (p. 4-77)

---

## 10 Fix the provisioning inconsistencies flagged by the `fephGrowth -m` command

Ensure that the configuration inconsistencies are resolved before the `fephGrowth -s` command is executed.

---

## 11 Execute a network switch

Execute the command `fephGrowth -s -w <worksheet file name>`.

**Note:** This procedure changes the packet path from an uplink on the Malban to an uplink on the DHSPP4M2 AMC. This results in the packet path going through the FEPH.

The parameter **<worksheet file name>** is the Signaling Firewall growth worksheet generated on execution of the command **fephGrowth -p**. The Signaling Firewall growth worksheet is populated with default gateway, static route, and NI type change specifications.

**Result:** The execution of network switch results in the following:

- Installation of static routes and default gateways for each IMS, H.248 and FS5K service as specified in the Signaling Firewall growth worksheet.
- Each IMS service is verified for FEPH readiness with appropriate FEPH routes.
- The IMS service is switched, resulting in an FEPH-enabled IMS service.
- The transport interfaces on the FEPH external access subnets are changed to HSPP4 ports.
- The “Unassigned” NI IP addresses on the FEPH service are assigned to “Published” NI.

**Note:** During a network switch, the configuration changes dynamically.

Execute the command **fephGrowth -m** to verify the resulting IMS service static routes, default gateways, and NI types.

Check for warning or error messages resulting from execution of the **fephGrowth -m** command.

---

## 12 Verify the UE ability to register and make calls on the FEPH-enabled IMS services

Verify if the user can register and make calls with the SIP signaling traversing the FEPH. If live traffic is present at the time of the **fephGrowth -s** execution, this verification can be performed by observing continuing live traffic.

---

## 13 Soak the new Signaling Firewall-based configuration

The new Signaling Firewall-based configuration is allowed to soak, serving either live or test traffic. The soak interval will end when it is established that the new Signaling Firewall-based configuration is performing correctly.

To execute the “Undo” procedure, proceed to [Step 14](#)

OR

On successful completion of the soak interval, execute the command **fephGrowth -a commit** and proceed to [Step 15](#)

---

**14 To execute the “Undo” procedure, contact the Tier 4 technical support representatives.**

**Note:** It is recommended that the “Undo” procedures are executed with the help of Tier 4 technical support representatives. The “Undo” procedures are used only if execution of the **fephGrowth -s** command results in network problems and the previous configuration has to be restored.

**Note:** The “Undo” procedures are service-impacting, with an estimated downtime of 10 min for hardware reboot and an additional 10 min for the IMS service to recover from a duplex failure.

---

**15 Perform a Signaling Firewall growth cleanup**

To perform a Signaling Firewall growth cleanup, see: “FEPH growth cleanup” (p. 5-200)

---

END OF STEPS

---

# To grow Signaling Firewall and FEPH on a new network

## Purpose

This topic describes the procedure to grow Signaling Firewall and FEPH on a new network.

## Prerequisite

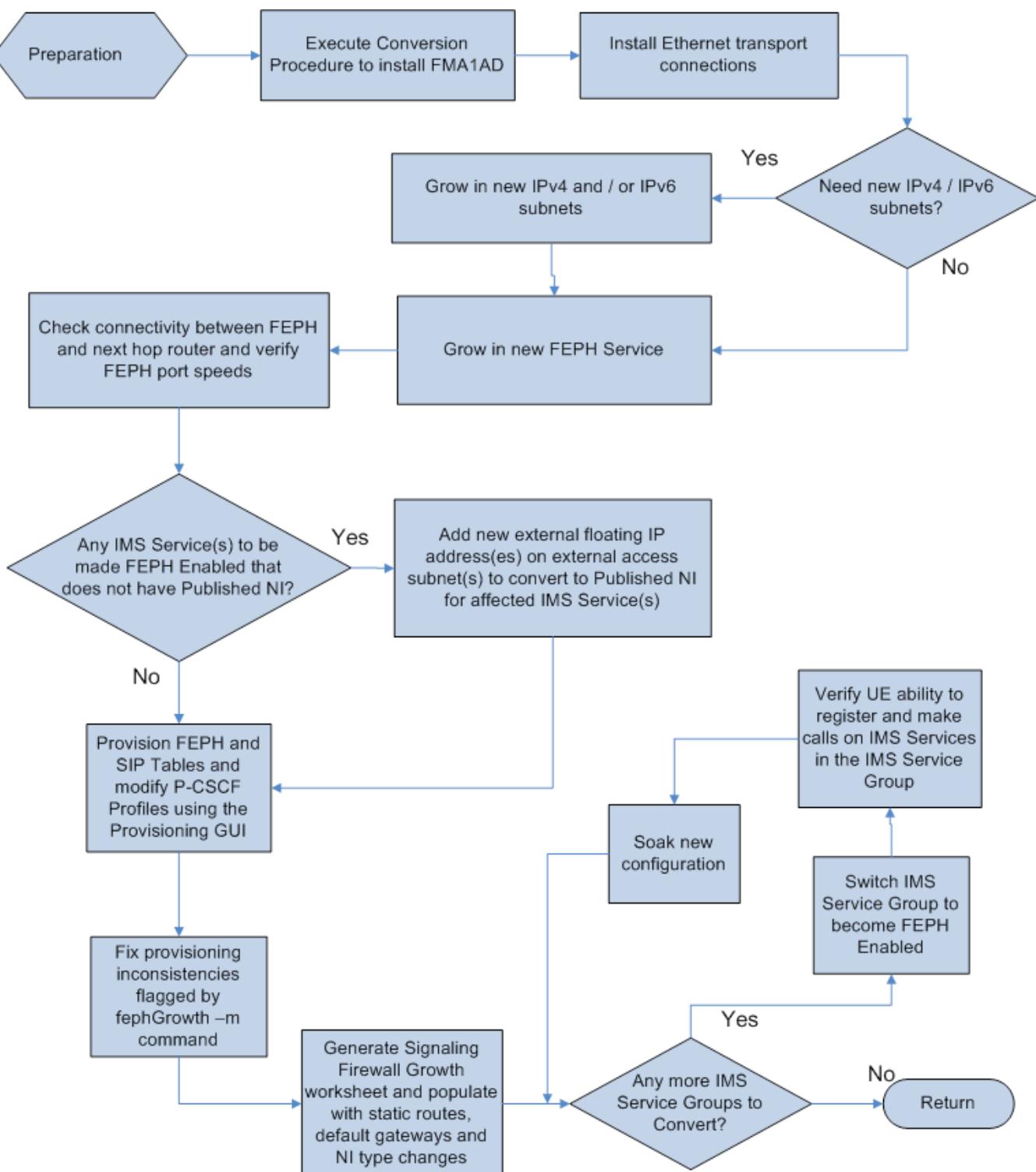
Before a group of IMS Services are switched to become FEPH-Enabled, the IMS Services must be shut down (with the service state “Out of Service”) so that at the time of the switch no subscribers are being served.

## Before you begin

**Note:** Ensure that the following procedure is executed: “[Signaling Firewall growth preparation and planning](#)” (p. 5-173).

**Note:** For information on error-handling during Signaling Firewall growth procedures, see: “[FEPH growth error-handling](#)” (p. 5-211)

The following figure shows the flow of Signaling Firewall growth operation using newly added external access subnets:



## Procedure

Perform the following steps:

### 1 Preparation

Following are the preparation steps to grow Signaling Firewall and FEPH on to new networks:

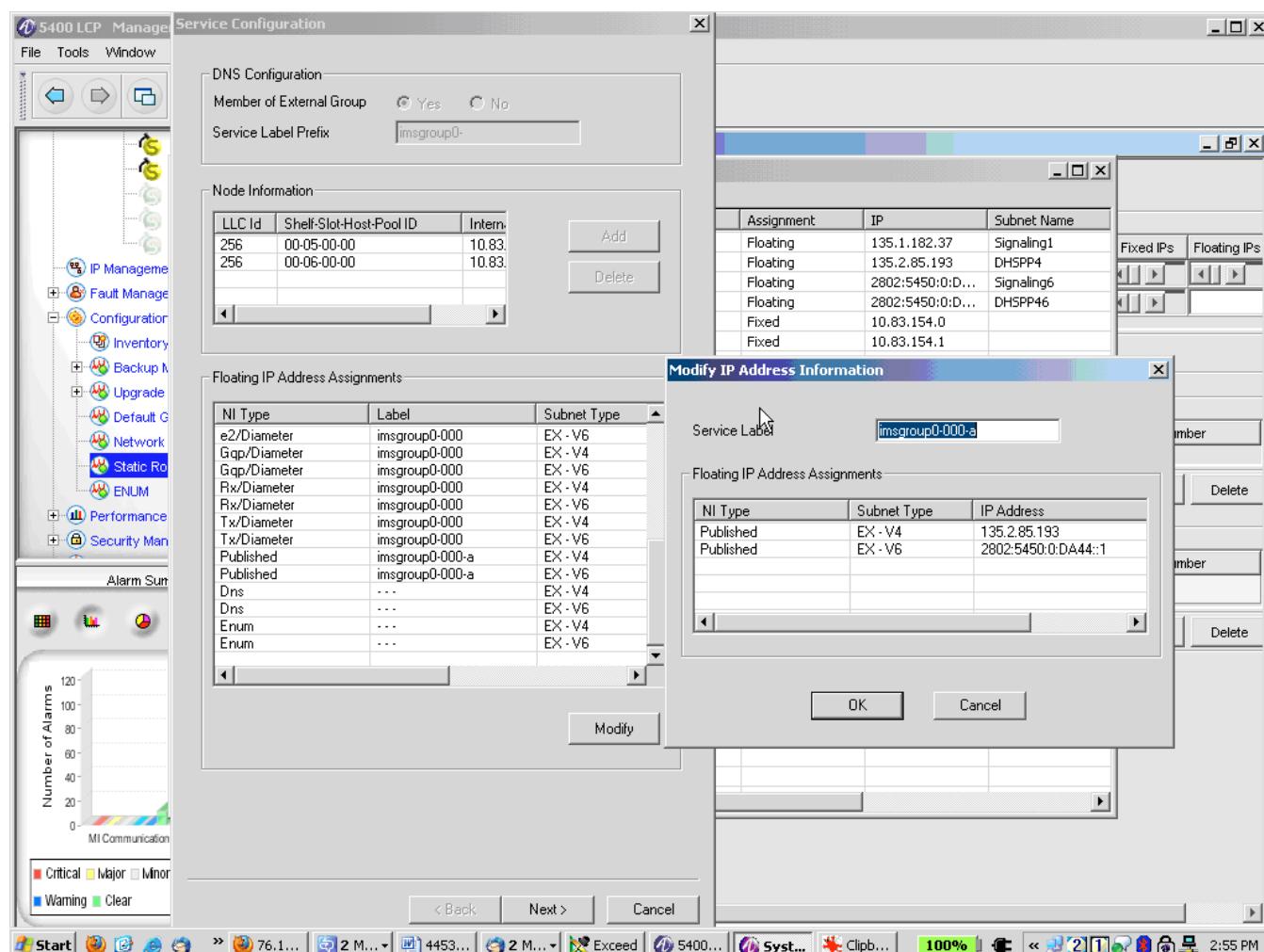
- Identify the IMS services to be FEPH-enabled. If multiple IMS services are present on a host and they are to be FEPH-enabled, group the IMS services before switching to minimize the number of service interruptions.
- For each IMS service group to be FEPH-enabled, plan the new static route and default gateway configuration. The new static route ensures that only the desired signaling traffic is routed through FEPH and prevents other signaling traffic (for example, DNS, diameter traffic, and so on) through the FEPH.

The identification of existing static routes and default gateways is obtained when executing the “[Signaling Firewall growth preparation and planning](#)” (p. 5-173) procedure.

The static routes override routing provided by the default gateway. If the Default Gateway routes messages through the FEPH, static routes could be defined for signaling that is not directed to the UEs through the access networks. For example, static routes can be defined for diameter, DNS, or ENUM signaling.

- The output of the command `fephGrowth -m` executed in the Signaling Firewall growth preparation and planning procedure displays the service label for each original Published NI on the IMS services. Preserve the service label information when the Published NI is moved to a new subnet. This information is used to restore the original service label value if the value of the original service label is changed during the growth procedure.

The original service label value can be restored using the following screen:



## 2 Execute the conversion procedure to install FMA1AD

For information on the conversion procedure, see, *Alcatel-Lucent 5400 Linux Control Platform Configuration Guide*, 270-702-014 Chapter 7Platform hardware conversion section *Platform hardware conversion*.

## 3 Install Ethernet transport connections

To install Ethernet transport connections between HSPP4 face plate and the external network equipment, see *Alcatel-Lucent 5400 Linux Control Platform Configuration Guide*, 270-702-014 Chapter 5Manage system configuration – hardware growth section *Growth system preparation*.

---

#### 4 Add new IPv4 or IPv6 subnets

For detailed procedures, see:

*Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014, Chapter: Manage system configuration - IP configuration, Section: IP address and route configuration, Topics: To add a new external IPv4 subnet and To add a new external IPv6 subnet.*

---

#### 5 Grow in a new FEPH service

To grow in a new FEPH service see: “[Service growth of FEPH service on HSPP4 of Malban \(Hub\) card](#)” (p. 5-201)

**Note:** The FEPH addresses must be assigned to the NI type “Published”.

---

#### 6 Check the connectivity between FEPH and the next hop router. Verify the FEPH port speeds.

Ensure that the connectivity between FEPH and the next hop router is properly established.

Check the following:

- Ensure proper physical connections to the next hop router exist.
- Proper configuration of FEPH service and next hop router exist.

The command **fephGrowth -c** is provided to verify proper communication.

**Note:** Before proceeding with subsequent growth steps:

- Ensure that a successful result is obtained on execution of the command **fephGrowth -c**.
- Verify the connection speed output. The maximum speed is 1Gigabit. The speed could be lower depending on the L2 router that the FEPH is connected to. The current connection speeds are displayed near the end of the **fephGrowth -c** output.

**Example:** Below is a sample output obtained on execution of the command

**fephGrowth -c:**

```
> ./fephGrowth -c
fephGrowth: started 08/11/10 07:33
Verifying config host (10.82.194.0) is reachable
config host (10.82.194.0) ping test completed successfully
fephGrowth: Inhibiting MI switchover
RCCavcmInhibitAdm: Request succeeded
fephGrowth: MI switchover now inhibited
fephGrowth Process conncheck request
```

```
=====Checking the connectivity for
IPv4=====
FEPH is enabled on subnet 9 for ipv4
Running tests to check connectivity for all hosts
chk_new_connectivity: Connectivity check was successfull.
chk_new_connectivity completed successfully
SU Health check completed successfully
=====Checking the connectivity for
IPv6=====
FEPH is enabled on subnet 10 for ipv6
Running tests to check connectivity for all hosts
chk_new_connectivity: Connectivity check was successfull.
chk_new_connectivity completed successfully
SU Health check completed successfully
host = cpr02-s00c07h4, ipd_port = 0, Name = eth2 (up), PortType =
external, PortSpeedInst =
1000000000
host = cpr02-s00c07h4, ipd_port = 1, Name = eth3 (up), PortType =
external, PortSpeedInst =
1000000000
host = cpr02-s00c08h4, ipd_port = 0, Name = eth2 (up), PortType =
external, PortSpeedInst =
1000000000
host = cpr02-s00c08h4, ipd_port = 1, Name = eth3 (up), PortType =
external, PortSpeedInst =
1000000000
fephGrowth: Re-enable MI RCC switchover
RCCavcmInhibitAdm: Request succeeded
fephGrowth: Re-enabled MI switchover
fephGrowth: Completed Successfully.
fephGrowth ended 08/11/10 07:34
```

## 7 Add new external floating IP addresses on external access subnets

If an IMS Service that is to be made FEPH-Enabled does not yet have a Published NI, then new external floating IP addresses (assigned to the Published NI) must be added to that IMS Service.

**Note:** A new Published NI must not be added to an IMS Service that already hosts P-CSCF SIPia ports.

For detailed procedures on how to add new external floating IP addresses, see *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014, chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add a new external floating IPv4 address* and *Alcatel-Lucent 5400 Linux Control Platform Configuration management guide*, 270-702-014 chapter: *Manage system configuration - IP configuration*, section: *IP address and route configuration*, topic: *To add a new external floating IPv6 address*.

---

## 8 Provision FSGUI FEPH and SIP Tables and modify P-CSCF Profiles

Perform the following:

- Populate the FEPH Tables data (IMS -> FEPH Tables). For more information on how to populate FEPH tables, see “[Provision the Signaling Firewall](#)” (p. 1-62). This must be done after the FEPH service is grown. The FEPH service growth step results in the automatic creation of FEPH default data.
  - Add iSGW policy and profile entries in the SIP tables (SIP Trusted Rate Limit Rule Set, SIP Untrusted Rate Limit Rule Set, Source Address Policy entries and Security Gateway Profile entries). This includes populating the FEPH Policies section of the applicable Security Gateway Profile entries. For more information on provisioning, see “[Provision Integrated Security Gateway \(iSGW\)](#)” (p. 1-51)
  - Modify the existing P-CSCF profile used on intended FEPH-enabled IMS services and/or the iSGW profile entries that are referenced from the P-CSCF.
- 

## 9 Fix the provisioning inconsistencies flagged by the `fephGrowth -m` command

Ensure that the configuration inconsistencies are resolved before the `fephGrowth -s` command is executed.

---

## 10 Populate the worksheet with static routes, default gateways, and NI changes

The user must begin looking at the worksheet and the network immediately. There is some delay between replacing the HUB with an FMA1AD version and doing the subsequent “worksheet” step.

To populate the worksheet with static routes, default gateways, and NI changes, see: “[FEPH growth worksheet](#)” (p. 5-212)

---

## 11 Switch the IMS service group

**Note:** Before this step is executed, ensure that the service state of the IMS services to be switched is “Out of Service”, so that at the time of switch no subscribers are being served.

Ensure that the MI and CNFG services are active on the same blade.

Execute the command:

`fephGrowth -g -w <seal growth worksheet> -l <pool list>`

The parameter **<seal growth worksheet>** is the Signaling Firewall growth worksheet generated on execution of the command **fephGrowth -p**. The Signaling Firewall growth worksheet is populated with default gateway, static route, and NI type change specifications. For more information on the Signaling Firewall growth worksheet, see: “[FEPH growth worksheet](#)” (p. 5-212)

The parameter **<pool list>** specifies a comma separated list of pool numbers for all the IMS services on a given host-pair to be FEPH-enabled.

**Note:** The pool list should not span multiple host-pairs.

**Result:** Execution of network switch results in the following:

- Modification of default gateways and static routes configuration as specified in the Signaling Firewall growth worksheet.
- Published NI IP addresses are moved to new external access subnets as specified in the Signaling Firewall growth worksheet.
- The IMS services are switched, resulting in FEPH-enabled IMS services.

**Note:** Unlock the IMS services to facilitate the verification of the UE ability to register and make calls.

After execution of the command **fephGrowth -g -w <seal growth worksheet> -l <pool list>**, compare the service label values for the Published NIs with the original values that were displayed on execution of the command **fephGrowth -m**. If the values have changed, restore the original values.

For information on how to restore original values, see “[Procedure](#)” (p. 5-194).

Execute the command **fephGrowth -m** and verify the resulting IMS service static routes, default gateways, and NI types.

**Note:** Check for warning or error messages generated on execution of the **fephGrowth -m** command.

---

## 12 Verify the UE ability to register and make calls on the IMS services

Ensure that the user can register and make calls with the SIP signaling traversing the FEPH.

---

## 13 Soak the new Signaling Firewall-based configuration

The new Signaling Firewall-based configuration is allowed to soak, serving either live or test traffic. The soak interval ends when it is established that the new Signaling Firewall-based configuration is performing correctly.

To execute the “Undo” procedure, proceed to [Step 14](#)

**Note:** Only one level of undo is supported. For example, if the user has already executed `fephGrowth -a commit` after executing `fephGrowth -g`, then the **Undo** option is not available.

OR

On successful completion of the soak interval, execute the command:

`fephGrowth -a commit` and proceed to **Step 15**

---

**14 To execute the “Undo” procedure, contact the Tier 4 technical support representatives.**

**Note:** It is recommended that the “Undo” procedures are executed with the help of Tier 4 technical support representatives. The “Undo” procedures are used only if problems are detected during the soak interval. An “Undo” operation reverts to the most recent change.

---

**15 Perform a Signaling Firewall growth cleanup**

To perform the Signaling Firewall growth cleanup, see: “[FEPH growth cleanup](#)” ([p. 5-200](#))

Repeat **Step 11** for other IMS services that need to be FEPH enabled in the worksheet.

END OF STEPS

---

# FEPH growth cleanup

## Purpose

This cleanup procedure is performed after successful FEPH growth in an existing office.

**Note:** This cleanup procedure is performed after successful completion of the soak interval.

## Procedure

The user can choose to perform the either of the steps depending on the task required:

- 
- 1 To delete unused IP addresses, perform the following step:

*Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014, Chapter: Manage system configuration - IP configuration, Section: IP address and route configuration, Topics:*

- *To delete an external floating IPv4 address*
- *To delete an external floating IPv6 address.*

The unused IP addresses are a result of addition of new external floating IP addresses during the FEPH growth procedures.

---

- 2 To delete unused subnets perform the following step:

*Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014, Chapter: Manage system configuration - IP configuration, Section: IP address and route configuration, Topics:*

- *To delete an external IPv4 subnet*
- *To delete an external IPv6 subnet*

The unused subnets are a result of addition of new subnets during the FEPH growth procedures.

END OF STEPS

---

# Service growth of FEPH service on HSPP4 of Malban (Hub) card

## Purpose

This procedure is used for service growth of FEPH service on HSPP4 of Malban (Hub) card.

## Before you begin

Ensure the following:

- The system is stable
- Perform a system backup
- The following information is required for the service growth procedure:
  - FEPH Service type
  - IPv4 subnet number
  - Corresponding NI types
  - Offsets if chosen
  - Default gateway subnet number for IPv4 or IPv6
  - IPv6 subnet number
  - IPv6 IP address and corresponding NI types
  - Shelf number
  - Card number
  - Host number
- Root passwords for both Hubs and the SOL Password are known.

For more information, see topic *Prepare for pre-software patch -> System Backup: Preparation - II* in the *Alcatel-Lucent 5400 Linux Control Platform Software Maintenance*, 270-702-031.

## Procedure

Perform the following:

- 
- 1 Open two windows and from both windows, log into *MI-1 host* as *root*.
- 

- 2 Execute the following command to find the *MI with active VM* :

```
MIcmd state vc
> MIcmd state vc
state of MI virtual cluster is A - Active
```

---

state of MI host primary virtual machine is A - Active  
state of MI host alternate virtual machine is S - Standby

---

- 3 If the primary VM is not active, then switch by using the following command:

**MICmd switch vc**

> Complete RCCvcswitch successfully: Wait for State Change.  
..... MI virtual cluster switched over successfully

Verify that the primary VM is active by executing the following command:

**MICmd state vc**

---

- 4 Execute the following command to create the host table, which will be used by the SIM tool.

**create\_ht**

**Result:**

```
> create_ht
Wed Jan 19 10:21:49 CST 2011 create_ht
Wed Jan 19 10:21:49 CST 2011 Saving backup files under /var/opt/lib/
    mtce/data
Wed Jan 19 10:21:49 CST 2011 Wrote new /var/opt/lib/mtce/data/mtce_
    host.data
Wed Jan 19 10:21:49 CST 2011 Wrote new /var/opt/lib/mtce/data/mtce_
    host.layout
Wed Jan 19 10:21:49 CST 2011 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.data
Wed Jan 19 10:21:49 CST 2011 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.layout
Wed Jan 19 10:21:49 CST 2011 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.data
Wed Jan 19 10:21:49 CST 2011 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.layout
Wed Jan 19 10:21:49 CST 2011 Wrote new /var/opt/lib/mtce/data/mtce_
    def_lib.ksh
```

---

- 5 Execute the following command as *root*.

**health**

**Note:** Proceed further only if this command reports success. Errors MUST be resolved before you can proceed with this procedure. For further assistance on this tool, contact your technical support representative.

- 6** To Inhibit switch over of MI, execute the following command:

```
rcc_adm --action set_inhibit --host MI-1hostname
```

- 7** To check the status of RCC inhibit, execute the command:

```
rcc_adm --action disp_inhibit --host MI-1hostname
```

**Note:** For all the command examples, see the topic “To grow service of diskless hosts for multiple services” in the *Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014*, Chapter: *Manage system configuration - hardware growth*, Section: *Growth implementation*.

- 8** Grow the IPv4 and IPv6 addresses by executing the following command:

```
svcgrow
```

svcgrow is used for growing in a new FEPH service and assigning an IP to that service. IP assignment is done manually by entering an IP address to be used on a specific subnet. Care must be taken not to use a duplicate IP that is already used by another NE.

#### Result:

```
svcgrow is a tool used to prepare sim host files
/var/opt/tmp/svcgrow/var/opt/lib/mtce/data/mtce_host.data
/var/opt/tmp/svcgrow/var/opt/lib/mtce/data/mtce_tim.data
/var/opt/tmp/svcgrow/var/opt/lib/mtce/data/mtce_srv.data
/var/opt/tmp/svcgrow/var/opt/lib/mtce/data/mtce_system.data
for growing one service pair on the existing
cards. Enter the service type for the pair, and then
enter the shelf, card and host number for one of the
card pair.

You can use ^C (control-C) at any time to
safely abort this interactive script.

Side A of pair 1: Enter the SHELF number [0..1]: 0
side A of pair 1: Enter the CARD number [1..14]: 7
side A of pair 1: Enter the HOST number [0..4]: 4
HOST_A at001-s00c07h4 ...

Enter the SERVICE TYPE. The allowed service types are as follows:
cs
ss7
h248
ims
fs5k
feph
imux

Please Enter:feph
Do you config IPv4 for feph Service (y/n) ?
y
```

Here are the current IPv4 subnets:  
 IPv4 subnet number 0, subnet base 10.1.0.0, subnet name internal  
 IPv4 subnet number 1, subnet base 135.1.60.112, subnet name campus  
 IPv4 subnet number 2, subnet base 10.241.1.0, subnet name signal  
 IPv4 subnet number 3, subnet base 10.241.1.64, subnet name billing  
 IPv4 subnet number 4, subnet base 10.241.1.128, subnet name published  
 Enter IPv4 SUBNET ID for feph Service IP : 4  
 Valid NI\_Type for feph Service IP :  
 published,h248\_published  
 Enter comma separated IP NI Types for feph,enter return for  
 unassigned : published  
 Enter IPv4 address for pair 1 feph service: 10.241.1.130  
 Check ipaddress 10.241.1.130 on subnet 4  
 Do you config IPv6 for feph Service (y/n) ?  
 y  
 Here are the current IPv6 subnets:  
 IPv6 subnet number 5, subnet base 2500:0000:0000:0012:0000:0000:0000:  
 0000, subnet name campus6  
 IPv6 subnet number 6, subnet base 2500:0000:0000:0013:0000:0000:0000:  
 0000, subnet name signal6  
 IPv6 subnet number 7, subnet base 2500:0000:0000:0014:0000:0000:0000:  
 0000, subnet name billing6  
 IPv6 subnet number 8, subnet base 2500:0000:0000:0015:0000:0000:0000:  
 0000, subnet name published6  
 Enter IPv6 SUBNET ID for feph Service IP : 8  
 Valid NI\_Type for feph Service IP :  
 published,h248\_published  
 Enter comma separated IP NI Types for feph,enter return for  
 unassigned : published  
 Enter IPv6 address for pair 1 feph service: 2500:0000:0000:0015:0000:  
 0000:0000:0002  
 Check ipaddress 2500:0000:0000:0015:0000:0000:0000:0002 on subnet 8  
 You are now ready to begin sim. For example:  
 in window 1: sim --proc svcgrow --action apply  
 in window 2: tail -f /storage/sim/log/svcgrow/sim.log

---

**9** On the first active MI window, execute the command:

**sim --proc svcgrow --action apply**

**Result:**

```
sim --proc svcgrow --action apply
*****
Software Installation Manager
(SIM)
*****
rules file: /opt/LSS/share/sim/rules/svcgrow/svcgrow.xml
source data directory: /var/opt/tmp/svcgrow/var/opt/lib/mtce/data
data directory: /storage/sim/data/svcgrow
log file: /storage/sim/log/svcgrow/sim.log
```

```
*** WARNING ***
The sim 'svcgrow' procedure will be '(re)applied' from the beginning.
If you continue, no further actions will be allowed based on
the procedure's current state.
Ready to 'apply' the sim 'svcgrow' procedure from the beginning:
Continue? (y/n) y
Executing ' sim --proc svcgrow --action apply ...
To monitor the sim 'svcgrow' procedure's log file use:
tail -f /storage/sim/log/svcgrowsim.log
```

- 
- 10 On the second active MI window, execute the command:

```
tail -f /storage/sim/log/svcgrowsim.log
```

**Note:** The second window is used to monitor the SIM progress. If a failure occurs during the execution of the SIM, the SIM will initiate a “pause” and report the failure to the user via the log file. When this occurs, the user should correct the root cause of the error and resume the growth by typing **sim --proc svcgrow --action resume**.

**Note:** During the execution of the growth procedures, additional transient alarm conditions may be observed. The alarms clear without manual intervention. If the alarms do not resolve after 10 min, contact the next level of technical support.

---

- 11 Service growth successfully completed, the log file displays:

**Result:**

```
COMPLETED SIM PROCEDURE 'svcgrow apply'
```

---

- 12 Execute the following command to create the host table:

```
create_ht
```

---

- 13 Find the external IP address of the hubs and execute the following command:

```
hubconf_adm --action show_ssh_address4
```

---

- 14 SSH to Hub “8”. Login as *root* and enter the root password.
- 

- 15 Open SOL to *MI-1* and execute the following command:

```
console -s shelf number -c card number
```

---

- 16 Enter the SOL password.
-

- 
- 17 Execute the following command:

```
hub_adm -a update -s shelf number -c 7 --growth
```

---

- 18 Terminate SOL to *MI* and execute the sequence of characters:

```
~.
```

---

- 19 Logout from Hub “8”.
- 

- 20 SSH to Hub “7”. Login as *root* and enter the root password.
- 

- 21 Open SOL to *MI-1* and execute the following command:

```
console -s shelf number -c card number
```

---

- 22 Enter the SOL password.
- 

- 23 Execute the following command:

```
hub_adm -a update -s Shelf number -c 8 --growth
```

---

- 24 Terminate SOL to *MI* and execute the sequence of characters:

```
~.
```

---

- 25 Logout of Hub “7”.
- 

- 26 Verify if the changes are up to date and execute the following command:

```
hub_adm -a check_all
```

---

- 27 To perform RCC switchover, execute the following command:

```
rcc_adm --action clr_inhibit --host MI-1hostname
```

---

- 28 To check the status of RCC inhibit, execute the following command:

```
rcc_adm --action disp_inhibit --host MI-1hostname
```

---

- 29 Trigger MI-GUI rediscovery procedures.

**Note:** For the detailed procedures, see *Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014*, Chapter: *Manage system configuration - MI-GUI procedures*, Section: *Discovery and growth using the MI-GUI*.

**Note:** For all the command examples, see the topic “To grow service of diskless hosts for multiple services” in the *Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014*, Chapter: *Manage system configuration - hardware growth*, Section: *Growth implementation*.

- 
- 30** Perform health.

**health**

---

- 31** Perform system backup.

**Note:** For backup procedures, see the topic “To perform full system backup” in the *Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014*, Chapter: *Manage system configuration - hardware growth*, Section: *Growth setup*.

**E N D O F S T E P S**

---

# fephGrowth command

## Description

This command is used in the following Signaling Firewall and FEPH growth procedures:

- “Signaling Firewall growth preparation and planning” (p. 5-173)
- “To grow Signaling Firewall and FEPH on an existing network” (p. 5-179)
- “To grow Signaling Firewall and FEPH on a new network” (p. 5-191)

## Tasks

Use this command to perform the following tasks:

- To print usage help information.
- To run the fephGrowth command in verbose mode. This option is helpful during debugging.
- To gather information on current configuration of the office.
- To generate the FEPH growth worksheet.
- To check the basic bi-directional connectivity between the FEPH service and the next hop router.
- To apply changes defined in the FEPH growth worksheet.

## Synopsis

```
fephGrowth [-v] -h|-m|-p|-c|-g -w <filename> -l <pool number list> | -s -w <filename>
```

This tool is designed to aid in the growth of FEPH into an existing office.

## Parameters

| Parameter            | Parameter definition                     |
|----------------------|--|
| <b>fephGrowth -h</b> | This option prints tool help information |

| Parameter  | Parameter definition   |
|--|--|
| <b>cephGrowth -m</b>   | <p>This option lists the detailed FEPH-related configuration information for the office and identifies configuration changes that must be made for a successful FEPH growth operation.</p> <p>On execution of this command the following list is generated:</p> <ul style="list-style-type: none"> <li>• Identification of all existing IMS services and SIPia ports configured in the office. This includes the external floating IP addresses being used to service the UE SIP traffic.</li> <li>• For each IMS service the configuration deficiencies to be fixed are identified.</li> <li>• All existing static routes and default gateways for each configured IMS, H.248 and FS5K services are identified.</li> <li>• All existing external subnets in the office are identified.</li> </ul> |
| <b>cephGrowth -p</b>   | Growth preparation. This option creates a growth worksheet showing information regarding default gateway, subnets, static routes and NI types.   |
| <b>cephGrowth -c</b>   | This option is used for FEPH IP connectivity check for both ipv4 and ipv6 address if any.  |
| <b>cephGrowth -g -w &lt;filename&gt; -l &lt;pool number list&gt;</b> | <p>FEPH growth to switch Service Group to FEPH enabled using worksheet.</p> <p><b>Note:</b> The pool numbers in -l list must not span multiple hosts.</p> <p>For example:</p> <pre><b>cephGrowth -g -w</b><br/><b>cephGrowthWorksheet.txt -l 1,2</b></pre> <p>In above example, pool number 1 and 2 must be on the same host.</p>  |
| <b>cephGrowth -s -w &lt;filename&gt;</b>                             | <p>This option is used for FEPH growth to switch Subnets to FEPH enabled using worksheet.</p> <p>For example:</p> <pre><b>cephGrowth -s -w</b><br/><b>cephGrowthWorksheet.txt</b></pre>  |

| Parameter                   | Parameter definition  |
|-----------------------------|---|
| <b>fephGrowth -a commit</b> | This option commits the current changes. The tool cannot restore once the commit is executed. |

# FEPH growth error-handling

This topic describes how to handle errors when executing a fephGrowth command.

## Recovery from fephGrowth command failure

The fephGrowth tool collects the SCDT configuration data before executing configuration changes during the FEPH growth procedures, so that the previous configuration can be restored in the event of a processing error. The log files and configuration data are collected and stored in the `/var/opt/log/fehpGrowth/error_snapshot.tar` file to aid in the investigation of the error handling.

If fephGrowth tool detects an error, the original configuration is automatically restored.

Listed below is an example of an error-handling event:

```
fehpGrowth: Error: IMS Services not all FEPH Ready (<CANDIDATE_STATUS>
NG:
No v4 (or potential v4) route through FEPH. PCSCF profiles must have
Security Gateway profiles with
FEPH policies. PCSCF profiles must have IPsec Secure ports = 0.</
CANDIDATE_STATUS>
<CANDIDATE_STATUS>NG: No v4 (or potential v4) route through FEPH.
PCSCF profiles must have Security Gateway profiles with FEPH policies.
PCSCF profiles must have IPsecSecure ports = 0.</CANDIDATE_STATUS>
<CANDIDATE_STATUS>NG: No v4 (or potential v4) route through FEPH.
PCSCF profiles must have Security Gateway profiles with FEPH policies.
PCSCF profiles must have IPsec
Secure ports = 0.</CANDIDATE_STATUS>
fehpGrowth: There was a failure in applying worksheet changes
fehpGrowth: Restoring SCDT config
/opt/LSS/sbin/scdm_adm --action restore_config --backupdir /var/opt/log/
fehpGrowth/backup_config
fehpGrowth commit_changes
/opt/LSS/sbin/netconf_adm --action generate_host_all
dat04-s00c01h0: generating network configuration... done
dat04-s00c02h0: generating network configuration... done
dat04-s00c05h0: generating network configuration... done
```

# FEPH growth worksheet

## FEPH growth worksheet

The FEPH growth worksheet is a *Microsoft Excel* worksheet in which the user can input data required during the FEPH growth process.

The worksheet is initially populated with the following data:

- Static route and default gateway data for each IMS, H.248 and FS5K services.
- NI Type data for each IMS service.
- External access subnet data.

The user can edit the worksheet to specify the required changes. The worksheet is used by the fephGrowth tool to automate the time-critical steps in the FEPH growth procedure.

## Procedure

- 1 Log in to the active MI host as *root* and execute the following command:

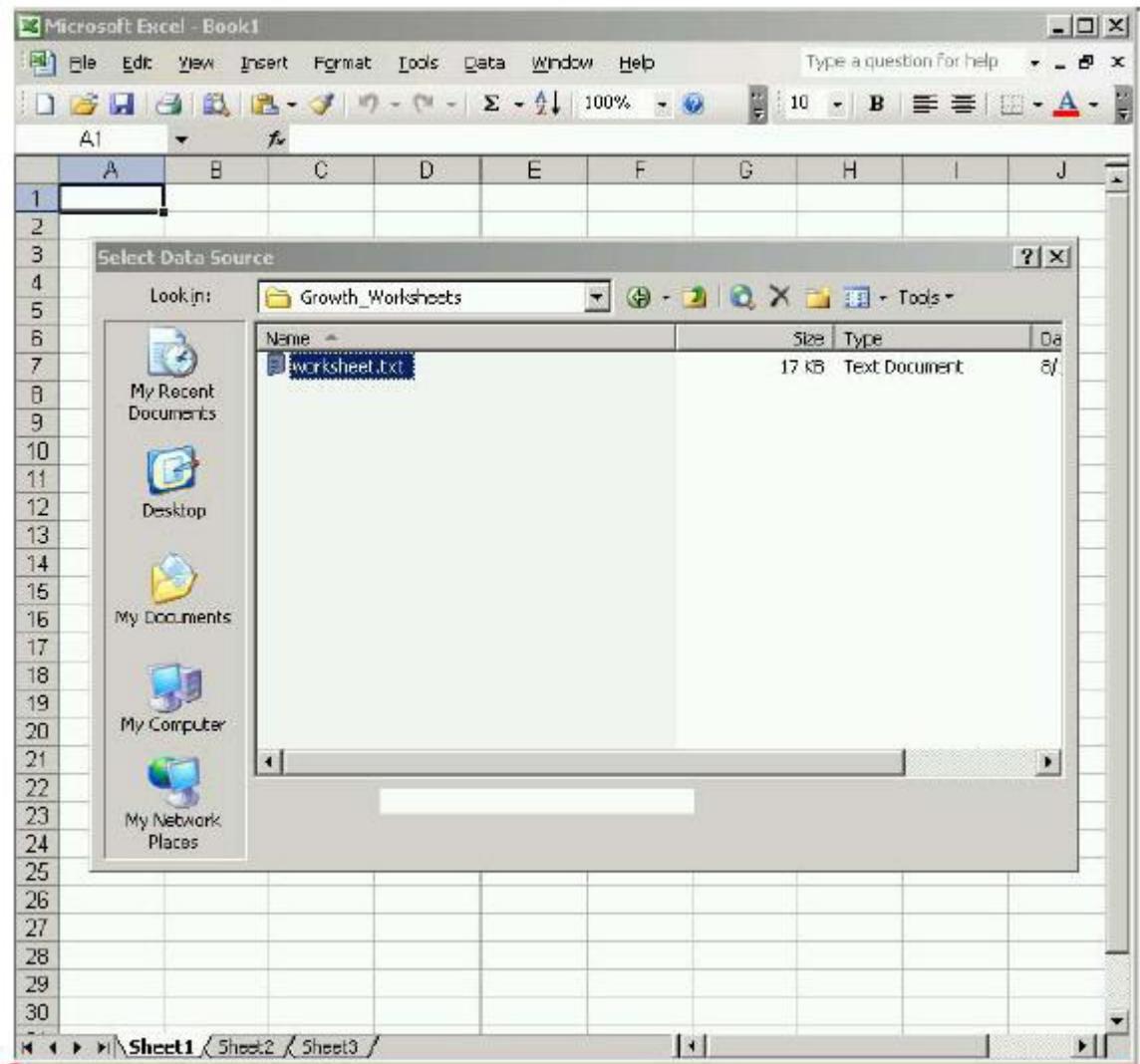
**fephGrowth -p**

**Example:** The resulting output can be found in the file */var/opt/log/fephGrowth/worksheet.txt*

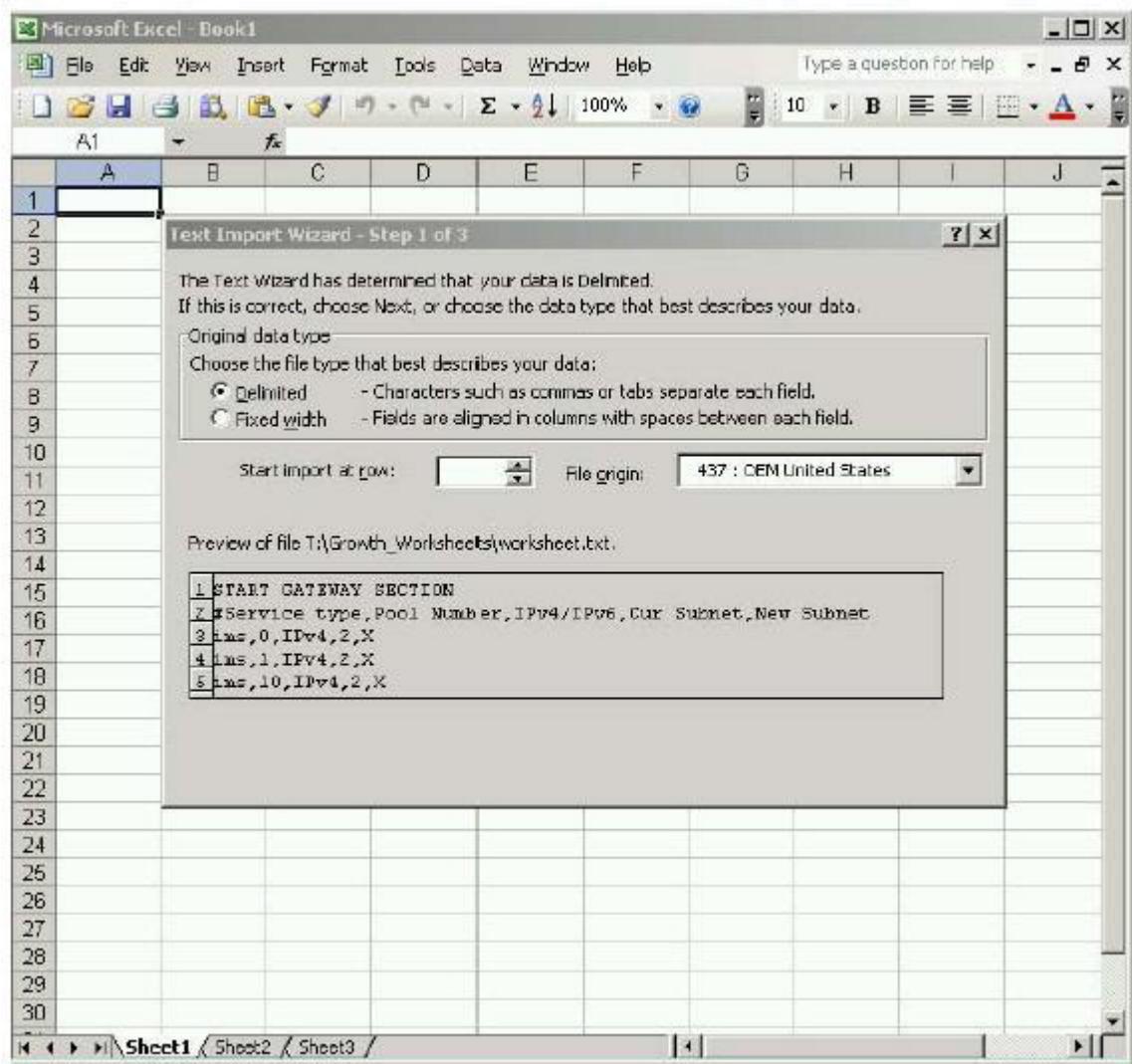
```
> fephGrowth -p
fephGrowth: started 08/12/10 13:51
Verifying config host (10.82.194.0) is reachable
config host (10.82.194.0) ping test completed successfully
fephGrowth: Inhibiting MI switchover
RCCavcmInhibitAdm: Request succeeded
fephGrowth: MI switchover now inhibited
fephGrowth Process prepcheck request
Exporting gateway information to worksheet...
Exporting subnet information to worksheet...
Exporting route information to worksheet...
Exporting NI type information to worksheet...
Export information to worksheet successful, worksheet file is:
/var/opt/log/fephGrowth/worksheet.txt
fephGrowth: Re-enable MI RCC switchover
RCCavcmInhibitAdm: Request succeeded
fephGrowth: Re-enabled MI switchover
fephGrowth: Completed Successfully.
fephGrowth ended 08/12/10 13:51
```

- 2 Load the file *worksheet.txt* into *Microsoft Excel* and execute the following sequence of commands in *Microsoft Excel*:

**Data -> Import External Data -> Import Data**

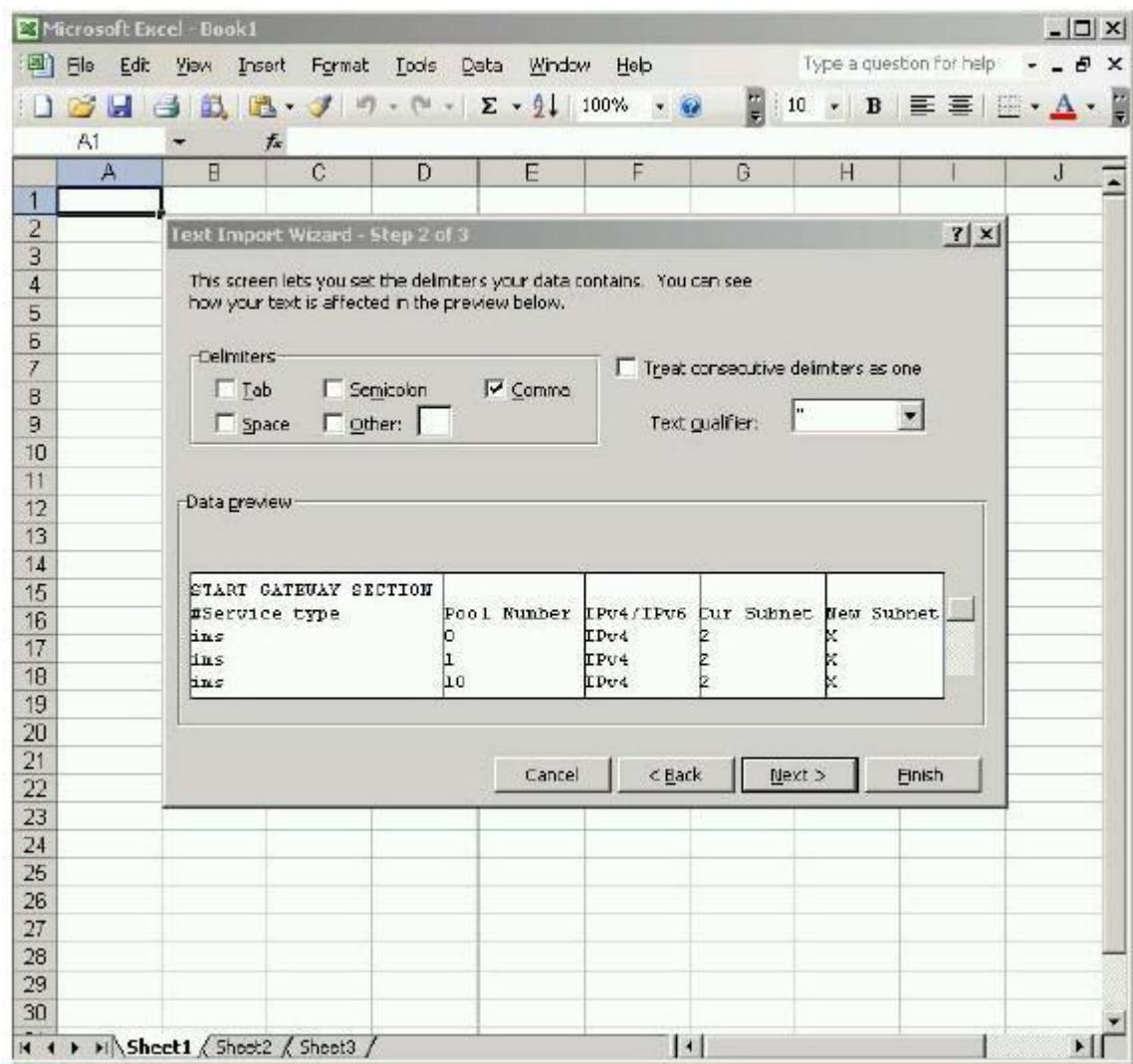
**Result:**

- 3 Specify that the input file *worksheet.txt* is “Delimited” and accept other defaults. Click the option “ **Next** ”.

**Result:**

- 
- 4 Specify the option “Comma” for De-limiters. Click the option “Next ”.

**Result:**



**5 Accept the default column data format**

**Result:**

This screen lets you select each column and set the Data Format.

'General' converts numeric values to numbers, date values to dates, and all remaining values to text.

Column data format:

General

Text

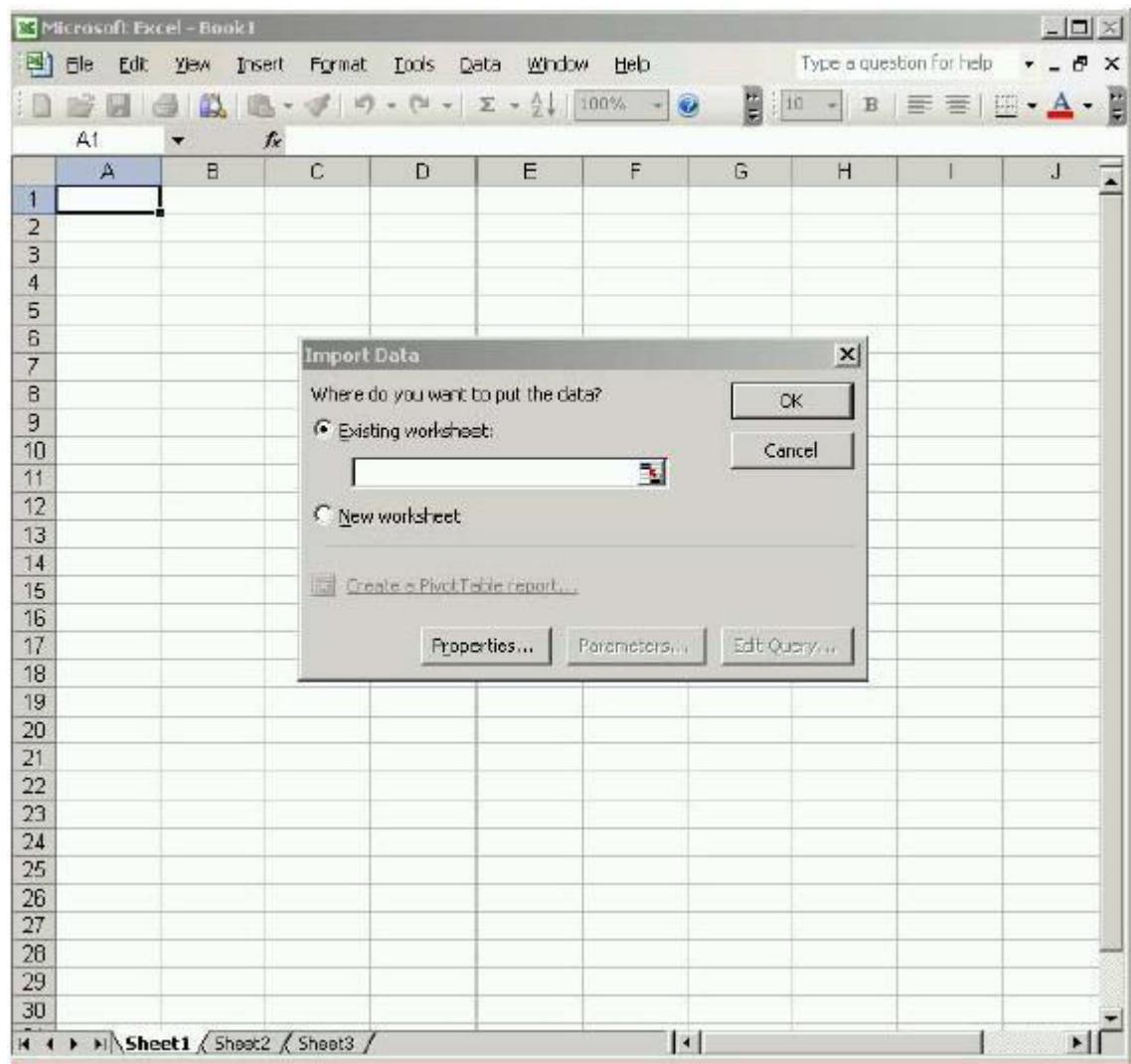
Date: MDY

Do not import column (skip)

advanced...

| General               | General       | General     | General   | General    |
|-----------------------|---------------|-------------|-----------|------------|
| START GATEWAY SECTION | #Service type | Pool Number | IPV4/IPv6 | Our Subnet |
| ims                   | ims           | 0           | IPv4      | X          |
| ims                   | ims           | 1           | IPv4      | X          |
| ims                   | ims           | 10          | IPv4      | X          |

- 
- 6 Accept the suggested placement of data.

**Result:**

- 7 The resulting *Microsoft Excel* sheet has four sections:

- Gateway section
- Subnet section
- Route section
- NI type section

**Result:**

| Microsoft Excel - Worksheet Sample for QDI-44537.xls |                             |                |           |            |
|--|-----------------------------|----------------|-----------|------------|
| START GATEWAY SECTION                                |                             |                |           |            |
| A  | B                           | C              | D         | E          |
| 1  | START<br>GATEWAY<br>SECTION |                |           |            |
| 2  | #Service type               | Pool<br>Number | IPv4/IPv6 | Cur Subnet |
| 3  | ims                         | 0              | IPv4      | 2 X        |
| 4  | ims                         | 1              | IPv4      | 2 X        |
| 5  | ims                         | 10             | IPv4      | 2 X        |
| 6  | ims                         | 11             | IPv4      | 2 X        |
| 7  | ims                         | 12             | IPv4      | 2 X        |
| 8  | ims                         | 13             | IPv4      | 2 X        |
| 9  | ims                         | 14             | IPv4      | 2 X        |
| 10   | ims                         | 15             | IPv4      | 2 X        |
| 11   | ims                         | 16             | IPv4      | 2 X        |
| 12   |                             |                |           |            |
| 13   | fs5k                        | 0              | IPv6      | 3 X        |
| 14   | fs5k                        | 1              | IPv6      | 3 X        |
| 15   | ims                         | 0              | IPv6      | 3 X        |
| 16   | ims                         | 1              | IPv6      | 3 X        |
| 17   | ims                         | 10             | IPv6      | 3 X        |
| 18   | ims                         | 11             | IPv6      | 3 X        |
| 19   | ims                         | 12             | IPv6      | 3 X        |
| 20   | ims                         | 13             | IPv6      | 3 X        |
| 21   | ims                         | 14             | IPv6      | 3 X        |
| 22   | ims                         | 15             | IPv6      | 3 X        |
| 23   | ims                         | 9              | IPv6      | 3 X        |
| 24   | END GATEWAY<br>SECTION      |                |           |            |

|    |                         |                  |                          |                                     |
|----|-------------------------|------------------|--------------------------|-------------------------------------|
| 25 | #                       |                  |                          |                                     |
| 26 | START SUBNET<br>SECTION |                  |                          |                                     |
| 27 | #IPv4 Subnet            | Subnet<br>Number | Subnet Base              | Subnet Mask                         |
| 28 | OAM                     | 1                | 10.223.8.32              | 255.255.255.224                     |
| 29 | SIGAccess               | 2                | 135.1.183.32             | 255.255.255.224                     |
| 30 | SIGCore                 | 3                | 10.223.9.32              | 255.255.255.224                     |
| 31 | Billing                 | 4                | 10.223.7.32              | 255.255.255.224                     |
| 32 | SigDHSP4                | 9                | 135.1.184.32             | 255.255.255.224                     |
| 33 | #IPv6 Subnet            | Subnet<br>Number | Subnet Prefix            | Prefix Length                       |
| 34 | Sig6DHSP4               | 10               | 2802:5450:1:ca25:0:0:0:1 | 64 2802:5450:1:ca25::ffff:ffff:ffff |
| 35 | OAM6                    | 5                | 2802:5450:1:ca21:0:0:0:1 | 64 2802:5450:1:ca21::ffff:ffff:ffff |
| 36 | SIG6Access              | 6                | 2802:5450:1:ca22:0:0:0:1 | 64 2802:5450:1:ca22::ffff:ffff:ffff |
| 37 | SIG6Core                | 7                | 2802:5450:1:ca24:0:0:0:1 | 64 2802:5450:1:ca24::ffff:ffff:ffff |
| 38 | Billing6                | 8                | 2802:5450:1:ca23:0:0:0:1 | 64 2802:5450:1:ca23::ffff:ffff:ffff |
| 39 | END SUBNET<br>SECTION   |                  |                          |                                     |

| START ROUTE SECTION |              |             |           |                         |                       |               |                  |
|---------------------|--------------|-------------|-----------|-------------------------|-----------------------|---------------|------------------|
| #                   | Service Type | Pool Number | IPv4/IPv6 | Subnet Base/Prefix      | Netmask/Prefix Length | Subnet Number | add/delete /keep |
| 42                  | fs5k         | 0           | IPv4      | 10.10.100.49            | 255.255.255.255       |               | 2 keep           |
| 43                  | fs5k         | 1           | IPv4      | 10.10.100.51            | 255.255.255.255       |               | 2 keep           |
| 45                  | ...          |             |           |                         |                       |               |                  |
| 46                  | fs5k         | 1           | IPv4      | 10.10.120.81            | 255.255.255.255       |               | 4 keep           |
| 47                  | h248         | 0           | IPv4      | 10.10.100.49            | 255.255.255.255       |               | 2 keep           |
| 48                  | ...          |             |           |                         |                       |               |                  |
| 49                  | h248         | 0           | IPv4      | 10.10.120.86            | 255.255.255.255       |               | 2 keep           |
| 50                  | h248         | 0           | IPv4      | 10.10.120.87            | 255.255.255.255       |               | 2 keep           |
| 51                  | ims          | 0           | IPv4      | 10.10.100.49            | 255.255.255.255       |               | 2 keep           |
| 52                  | ims          | 0           | IPv4      | 10.10.100.51            | 255.255.255.255       |               | 2 keep           |
| 53                  | ims          | 0           | IPv4      | 10.10.120.115           | 255.255.255.255       |               | 2 keep           |
| 54                  | ims          | 11          | IPv4      | 10.10.120.116           | 255.255.255.255       |               | 4 keep           |
| 55                  | ims          | 11          | IPv4      | 10.10.120.117           | 255.255.255.255       |               | 4 keep           |
| 56                  | ims          | 14          | IPv4      | 10.10.120.115           | 255.255.255.255       |               | 4 keep           |
| 57                  | ims          | 14          | IPv4      | 10.10.120.116           | 255.255.255.255       |               | 4 keep           |
| 58                  | ims          | 14          | IPv4      | 10.10.120.117           | 255.255.255.255       |               | 4 keep           |
| 59                  | ims          | 0           | IPv6      | 2803:5450:1:a120:0:0:5a |                       | 128           | 6 keep           |
| 60                  | ims          | 0           | IPv6      | 2803:5450:1:a120:0:0:5b |                       | 128           | 6 keep           |
| 61                  | ims          | 0           | IPv6      | 2803:5450:1:a120:0:0:5c |                       | 128           | 6 keep           |
| 62                  | ims          | 1           | IPv6      | 2803:5450:1:a120:0:0:5a |                       | 128           | 6 keep           |
| 63                  | ims          | 1           | IPv6      | 2803:5450:1:a120:0:0:5b |                       | 128           | 6 keep           |
| 64                  | ims          | 1           | IPv6      | 2803:5450:1:a120:0:0:5c |                       | 128           | 6 keep           |
| 65                  | ims          | 2           | IPv6      | 2803:5450:1:a120:0:0:5a |                       | 128           | 6 keep           |
| 66                  | ims          | 3           | IPv6      | 2803:5450:1:a120:0:0:5c |                       | 128           | 6 keep           |
| 67                  | ims          | 4           | IPv6      | 2803:5450:1:a120:0:0:5a |                       | 128           | 6 keep           |
| 68                  | ims          | 4           | IPv6      | 2803:5450:1:a120:0:0:5b |                       | 128           | 6 keep           |
| 69                  | ims          | 4           | IPv6      | 2803:5450:1:a120:0:0:5c |                       | 128           | 6 keep           |
| 70                  | ims          | 8           | IPv6      | 2803:5450:1:a120:0:0:5c |                       | 128           | 6 keep           |
| 71                  | ims          | 9           | IPv6      | 2803:5450:1:a120:0:0:5a |                       | 128           | 6 keep           |
| 72                  | ims          | 9           | IPv6      | 2803:5450:1:a120:0:0:5c |                       | 128           | 6 keep           |
| END ROUTE SECTION   |              |             |           |                         |                       |               |                  |
| 73                  |              |             |           |                         |                       |               |                  |

| START NITYPE SECTION |                      |             |           |   |                     |                   |
|----------------------|----------------------|-------------|-----------|---|---------------------|-------------------|
|                      | A                    | B           | C         | D   | E                   | F                 |
| 75                   | START NITYPE SECTION |             |           |   |                     |                   |
| 76                   | #Nl_Type             | Pool Number | IPv4/IPv6 | Subnet Number                             | IPv4_Offset/IPv6_IP | New Subnet Number |
| 77                   | diam_rf              | 0           | Pv4       | 4   |                     | 1 X               |
| 78                   | default              | 0           | Pv4       | 3   |                     | 6 X               |
| 79                   | published            | 0           | Pv4       | 2   |                     | 11 X              |
| 80                   | diam_rf              | 10          | Pv4       | 4   |                     | 11 X              |
| 81                   | default              | 10          | Pv4       | 3   |                     | 16 X              |
| 82                   | ...                  |             |           |   |                     |                   |
| 83                   | published            | 14          | Pv4       | 2   |                     | 24 X              |
| 84                   | diam_rf              | 15          | Pv4       | 4   |                     | 16 X              |
| 85                   | default              | 15          | Pv4       | 3   |                     | 21 X              |
| 86                   | ...                  |             |           |   |                     |                   |
| 87                   | published            | 6           | Pv4       | 2   |                     | 18 X              |
| 88                   | diam_rf              | 7           | Pv4       | 4   |                     | 8 X               |
| 89                   | default              | 7           | Pv4       | 3   |                     | 13 X              |
| 90                   | published            | 7           | Pv4       | 2   |                     | 17 X              |
| 91                   | ...                  |             |           |   |                     |                   |
| 92                   | published            | 0           | Pv6       | 6 2802:5450:0001:ca22:0000:0000:0000:00 X |                     | X                 |
| 93                   | diam_rf              | 0           | Pv6       | 8 2802:5450:0001:ca23:0000:0000:0000:00 X |                     | X                 |
| 94                   | default              | 0           | Pv6       | 7 2802:5450:0001:ca24:0000:0000:0000:00 X |                     | X                 |
| 95                   | published            | 10          | Pv6       | 6 2802:5450:0001:ca22:0000:0000:0000:00 X |                     | X                 |
| 96                   | ...                  |             |           |   |                     |                   |
| 97                   | published            | 14          | Pv6       | 6 2802:5450:0001:ca22:0000:0000:0000:00 X |                     | X                 |
| 98                   | diam_rf              | 14          | Pv6       | 8 2802:5450:0001:ca23:0000:0000:0000:00 X |                     | X                 |
| 99                   | default              | 14          | Pv6       | 7 2802:5450:0001:ca24:0000:0000:0000:00 X |                     | X                 |
| 100                  | published            | 15          | Pv6       | 6 2802:5450:0001:ca22:0000:0000:0000:00 X |                     | X                 |
| 101                  | ...                  |             |           |   |                     |                   |
| 102                  | diam_rf              | 8           | Pv6       | 8 2802:5450:0001:ca23:0000:0000:0000:00 X |                     | X                 |
| 103                  | default              | 8           | Pv6       | 7 2802:5450:0001:ca24:0000:0000:0000:00 X |                     | X                 |
| 104                  | published            | 9           | Pv6       | 6 2802:5450:0001:ca22:0000:0000:0000:00 X |                     | X                 |
| 105                  | diam_rf              | 9           | Pv6       | 8 2802:5450:0001:ca23:0000:0000:0000:00 X |                     | X                 |
| 106                  | default              | 9           | Pv6       | 7 2802:5450:0001:ca24:0000:0000:0000:00 X |                     | X                 |
| 107                  | END NITYPE SECTION   |             |           |   |                     |                   |

The purpose of each section in the *Microsoft Excel* sheet is described below:

| Section   | Purpose  |
|---|--|
| Gateway section<br><br><b>Note:</b> Gateway changes apply to all services (IMS, H.248 and FS5K) on a host. Therefore, if a gateway for IMS Services is changed to cause default traffic to traverse the FEPH, routes need to be added for H.248 and FS5K to prevent their signaling traffic from traversing the FEPH. | Populate the New subnet column entry (that is, replace the X) for any IMS service to change the IPv4 or IPv6 default gateway subnet. |
| Subnet section  | This section is only for reference. It identifies the IPv4 or IPv6 external subnets and provides the subnet numbers.                 |

| Section   | Purpose   |
|---|---|
| Route section<br><br><b>Note:</b> Route changes apply to all services (IMS, H.248 and FS5K) on a host. Therefore, if a gateway for IMS Services is changed to cause default traffic to traverse the FEPH, routes need to be added for H.248 and FS5K to prevent their signaling traffic from traversing the FEPH. | Add IPv4 or IPv6 static routes by adding new entries to the section and populate them with the keyword “Add” in the “Add/Delete/Keep” column.<br><br>To remove a static route, change the keyword in the “Add/Delete/Keep” column to “Delete”.  |
| NI type section   | To move the Published NI for an IMS service to new external access subnets and IP addresses by populating the “New subnet number” and “New offset or new IPv6 IP” columns.<br><br>This section is not used during the SEAL growth scenario during which existing external access subnets are used for the FEPH. |

8 On completion of modifications to the worksheet, save the resulting file in .csv format.

Use the menu option **File -> Save As** to save the file in .csv format.

9 Transfer the .csv file to the *root* login of the active MI host.

**Result:** The resulting file is used with **fephGrowth -s** or **fephGrowth -g** commands.

END OF STEPS

# Migration procedure for signaling firewall load balancer/distribution function

## Overview

### Purpose

This section describes the procedure to migrate IMS services to Signaling Firewall Load Balancer/Distribution function with single IP address exposed for the Gm Interface to end users.

### Contents

|  |       |
|--|-------|
| Migration Procedure for Signaling Firewall Load Balancer/Distribution Function | 5-223 |
|--|-------|

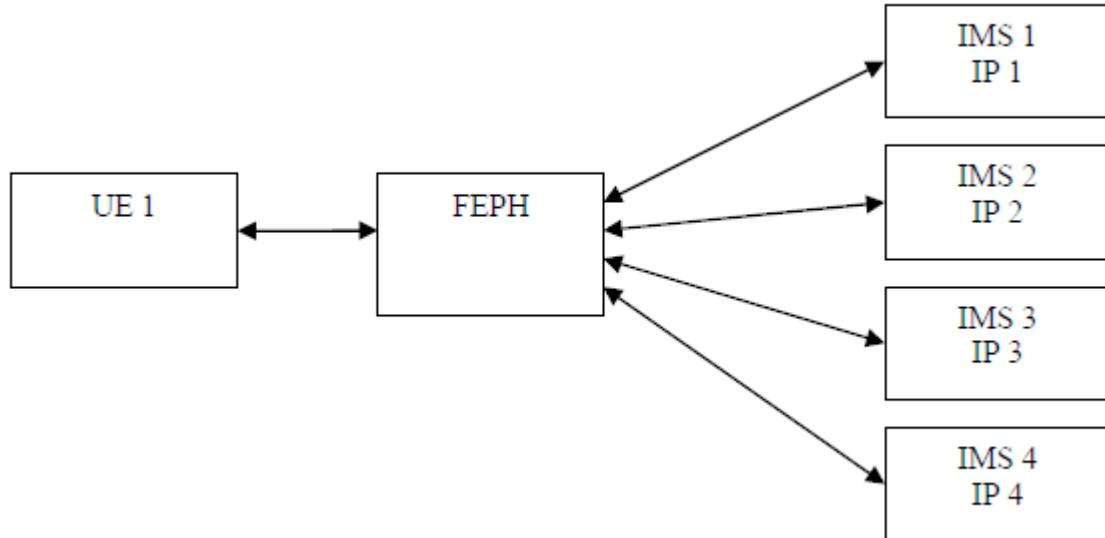
# Migration Procedure for Signaling Firewall Load Balancer/Distribution Function

## Overview

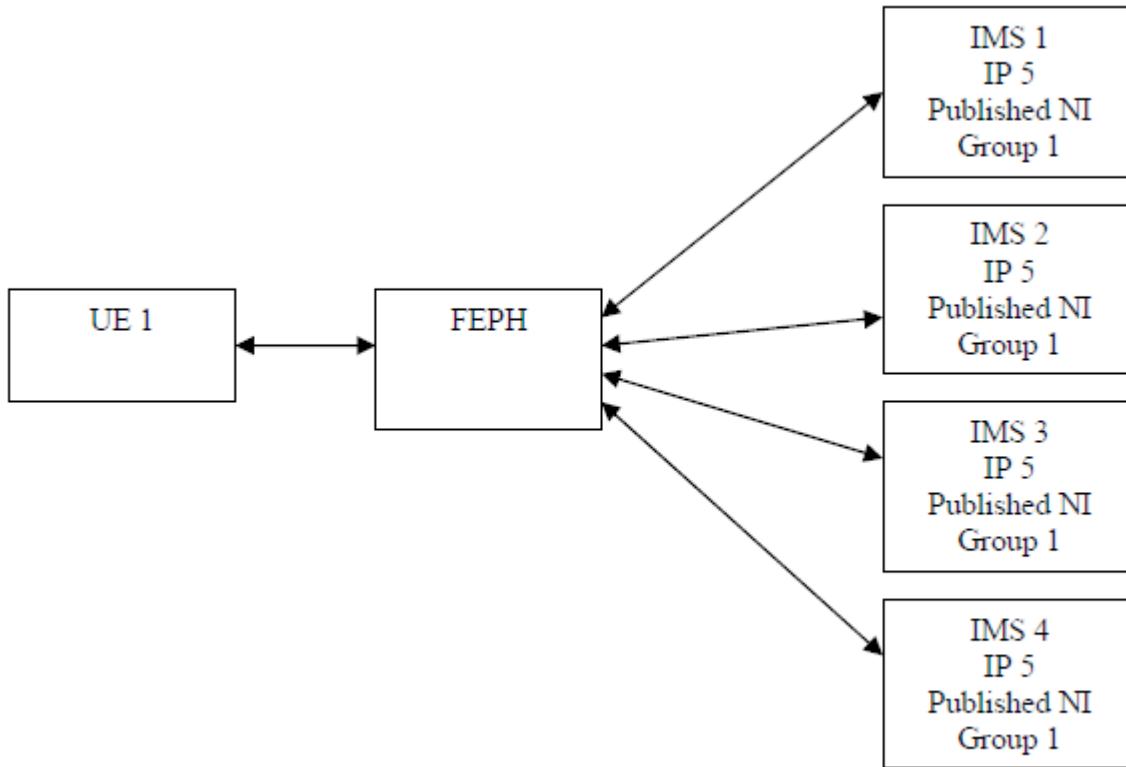
This procedure is used for migrating Signaling Firewall Load Balancer/Distribution function with single IP address exposed for the Gm Interface to end users.

## Description

The aim of migration to Distributed IP is to place existing FEPH enabled IMS services in a Published NI group. The following figure shows a typical IMS configuration where each IMS service has a unique IPv4/IPv6 address on the Gm interface.



The following figure shows the above configuration after the IMS services have been migrated to the distributed IP. Note that all the IMS services have the same IP address exposed on that Gm interface, and are all in the same Published NI Group. Also, this figure shows all of the original IMS services having a different IP (IP5) after migration. It is allowed that one of the IMS services retains the original IP and the other IMS services are migrated to that IP. For instance in the following figure, all IMS services can have IP1.



**The following conditions are to be met:**

- The Shared Published NI IP addresses must be on the FEPH external access subnet. This procedure assumes that all IMS services involved in the migration are already feph enabled.
- All IMS service instances within a Published NI Group must have a Published NI on the FEPH subnet with the same IPv4/IPv6 IP address combination, that means they cannot have different mixes of IPv4/IPv6 addresses.

For example, service instance 1 is assigned a published NI with IPv4 IP X/IPv6 IP Y and service instance 2 is assigned a published NI with IPv4 IPX/IPv6 IP Z.

- The Derived Service Labels for published NI can remain unique across services even if published IPs are shared.
- Migrating to or from shared Published NI IP addresses requires you to follow detailed procedures that involves both MI and provisioning operations. Simply changing a Published NI IP on the MI without following the procedures results in database corruption.

- Distributed IP means that there exists a Published NI group with more than one IMS service. The published NI groups can exist with a single IMS service but technically it is not considered to be a distributed IP until more than one IMS service uses the same Published IP on a FEPH external access subnet.
- A service instance can only appear in at most one published NI group.
- If a Published NI Group has more than one IMS service, then the service instance being inserted or deleted must not be FEPH Enabled. If the service being inserted or deleted is the only service in the group, then it can be FEPH enabled.

**Steps required to migrate to IMS services that *SHARE* the same Published IP on a FEPH enabled external access subnet**

**STEP - 1:** For each IMS service instance to be in the same Published NI Group, add the same new external floating IP addresses (IPv4 and/or IPv6) as “Unassigned” NI.

For detailed procedures, see the topics “To add a new external floating IPv4 address” and “To add a new external floating IPv6 address” in the *Alcatel-Lucent 5400 Linux Control Platform Configuration Management, 270-702-014* user manual.

This example adds an unassigned IPV4 external floating IP FEPH enabled access subnet 4 for the IMS services poolnum 2. The offset for the floating IP is 3. The base IP address for subnet 4 can be found using the following command:

- `net4conf_adm --action show_external_subnet`
- `ip_adm -a add_floating_ip -t ims -i 2 -s 4 -o 3 -r`
- `ip_adm -a commit`

This example adds an unassigned IPV6 external floating IP FEPH enabled access subnet 8 for the IMS services poolnum 2. The offset for the floating IP is 3. The prefix address for subnet 8 can be found using the following command

- `net6conf_adm --action show_external_subnet`
- `ip_adm -a add_floating_ip -t ims -i 2 -s 8 -o 2802:5450:1:a034::3 -r`
- `ip_adm -a commit`

**STEP - 2:** For each IMS service instance to be in the same Published NI Group, verify that the following preconditions are met and correct if not:

- All P-CSCFs in the Published NI Group with the same Port Number must have the same Port Name.
- All P-CSCFs in the Published NI Group with the same Port Name must have the same ACR Messages Generation, Allow Immediate 200 OK, and Area ID values.
- All P-CSCFs in the Published NI Group must use the same Service Based Profile.
- All P-CSCFs in the Published NI Group must have unique TLS Server Port Numbers.

- All P-CSCFs in the Published NI Group must not have TLS Server Port Numbers and “SIP” Port Numbers with the same value.
- P-CSCFs in the Published NI Group with the same Port Name can only have the same SIP Permanent Linkset Group Number if all the SIP Linksets in the group do not have any “Publish” NI 1 values.

**STEP - 3:** For each IMS service instance to be in the same Published NI Group:

1. If there is a shared unassigned floating IP for this IMS service (see **STEP - 1**):
  - a. Lock or Shutdown the IMS service and wait for the lock to complete.
  - b. Delete the IMS service from the FEPH Enabled IMS Services list.
  - c. On MI→Configuration Management→Network Interface, modify the published NI for the IMS service. Choose the shared unassigned floating IPv4/IPv6 addresses (see **STEP - 1**). See the example in the figure below. Unassigned IPs 135.1.69.162 and 2802:5450:0001:a034:0000:0000:0002 are also the floating IPs on the Published NI of IMS 0. Note, MI states that the service must be switched over for the change to be applied. This is done in the **STEP - 3**, fifth step.
2. If needed, delete the IMS service from the FEPH Enabled IMS Services list.
3. Add the IMS service to a new or existing Published NI Group table.
4. Add the IMS service to the FEPH Enabled IMS Services list.
5. If needed, switchover the IMS service.
6. If needed, unlock IMS service
7. Optionally, delete the unassigned floating IP from this IMS service. Note, after first step of **STEP - 3**, the previous Published IP will be made unassigned and can then be deleted.

Steps needed to migrate to FEPH enabled IMS services that *DO NOT SHARE* the same Published IP on a FEPH enabled access subnet.

**STEP - 1:** For each IMS service instance that is currently in the same Published NI Group, add new unique external floating IP addresses (IPv4 and/or IPv6) as “Unassigned” NI.

For detailed procedures, see the topics “To add a new external floating IPv4 address” and “To add a new external floating IPv6 address” in the *Alcatel-Lucent 5400 Linux Control Platform Configuration Management*, 270-702-014 user manual.

This example adds an unassigned IPV4 external floating IP FEPH enabled access subnet 4 for the IMS services poolnum 2. The offset for the floating IP is 3. The base IP address for subnet 4 can be found using the following command

- `net4conf_adm --action show_external_subnet`
- `ip_adm -a add_floating_ip -t ims -i 2 -s 4 -o 3 -r`
- `ip_adm -a commit`

This example adds an unassigned IPV6 external floating IP FEPH enabled access subnet 8 for the IMS services poolnum 2. The offset for the floating IP is 3. The prefix address for subnet 8 can be found using the following command:

- `net6conf_adm --action show_external_subnet`
- `ip_adm -a add_floating_ip -t ims -i 2 -s 8 -o 2802:5450:1:a034::3 -r`
- `ip_adm -a commit`

**STEP - 2:** For each IMS service instance to be removed from the Published NI Group, verify that the following precondition is met and correct if not:

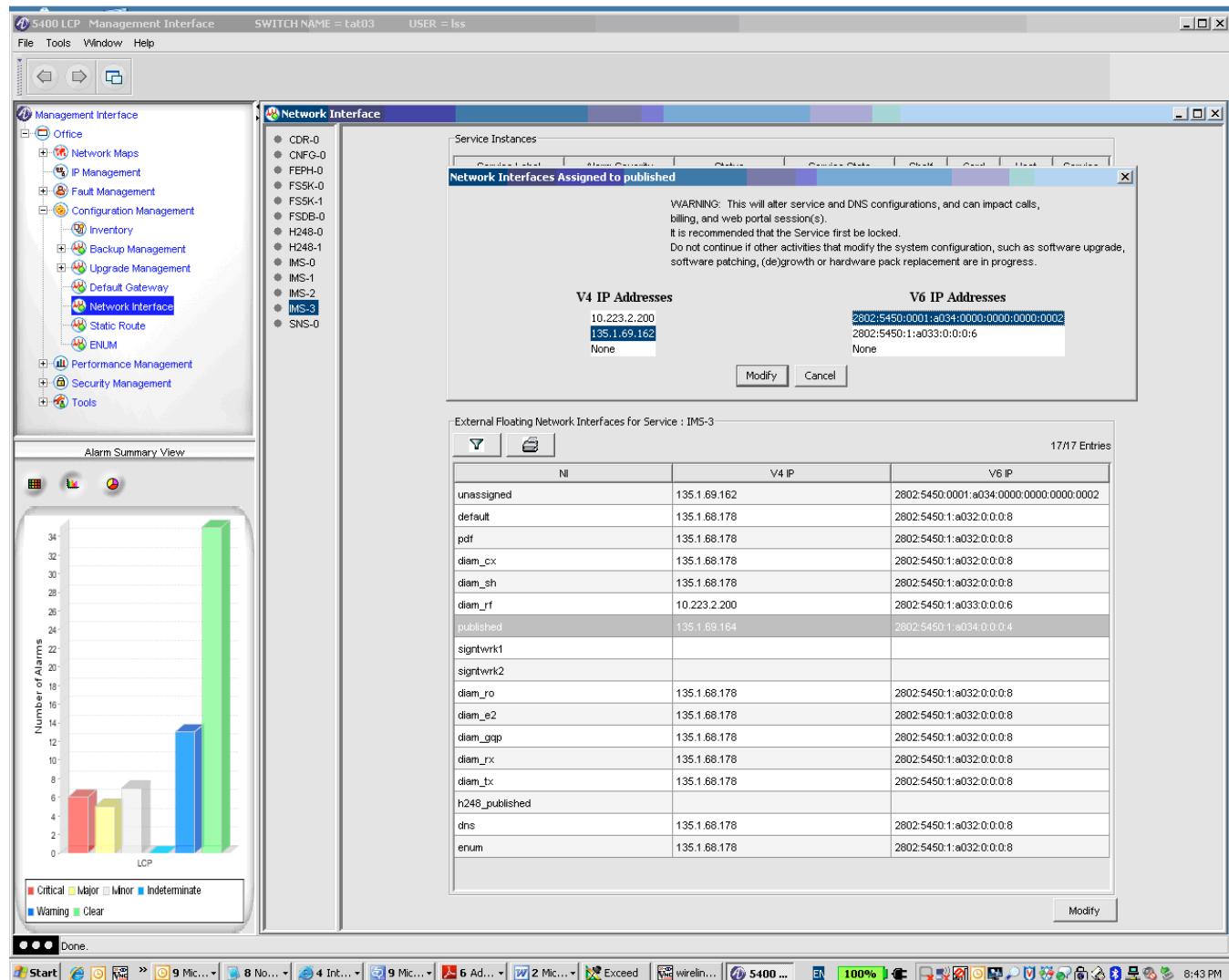
Any PCSCFs that exist on the affected service(s) whose Port Name matches existing PCSCFs on unshared IMS services must have the same Permanent Linkset Group Number (in order to confirm to cross checks).

**STEP - 3:** For each IMS service instance to be removed from the Published NI Group:

1. If there is a unique unassigned floating IP for this IMS service (see **STEP - 1**):
  - a. Lock/Shutdown the IMS service and wait for the lock to complete
  - b. Delete the IMS service from the FEPH Enabled IMS Services list.
  - c. Delete the IMS service from the Published NI Group table.
  - d. On MI->Configuration Management->Network Interface, modify the published NI for the IMS service. Choose the unique unassigned floating IPv4/IPv6 addresses (see **STEP - 1**). Note, MI will state that the service must be switched over for the change to be applied. This is done on **STEP - 3**, third step below.
2. If needed, add the IMS service to the FEPH Enabled IMS Services list.
3. If needed, switchover the IMS service.
4. If needed, unlock IMS service.
5. Optionally, delete the unassigned floating IP from this IMS service.

#### To modify the IP address(es) of FEPH enabled IMS services that currently SHARE the same Published IP on a FEPH enabled external access subnet -

In order to ensure that at least one IMS service is active at all times, it is recommended that the procedure above be followed to migrate the IMS services to FEPH enabled IMS services that DO NOT SHARE the same Published IP on a FEPH enabled access subnet. Then, follow the procedure above to migrate to IMS services that SHARE the same Published IP on a FEPH enabled external access subnet, using the new desired IP address(es).



# To provision signaling firewall load balancer or distribution function with single IP address exposed for the Gm interface to end users

DRAFT

## Overview

### Purpose

This section describes the provisioning procedures for Signaling Firewall Load Balancer or Distribution Function with Single IP Address Exposed for the Gm Interface to End Users.

### Contents

|  |       |
|--|-------|
| To provision a Published NI Group Assignment table | 5-230 |
|--|-------|

DRAFT

# To provision a Published NI Group Assignment table

## Purpose

This procedure is used to provision a Published NI Group Assignment table.

## Before you begin

This table is used to assign a valid IMS services to a Published NI group. The maximum number of tables that can be provisioned is 1. The maximum records per table is 64 (current maximum number of device server node IDs).

Any time an IMS service is being added or removed from this table, checks will be made to verify the existing PCSCF SIPia port data fields and also to verify the IMS service is not FEPH Enabled in the FEPH Enabled table.

Import/export table operations are not supported by the Published NI Group Assignment table.

## Steps to provision a Published NI Group Assignment table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS → FEPH Tables**.

**Result:** The **FEPH Tables** window is displayed.

---

- 2 In the left pane, expand the **Published NI Group Assignment** folder.

**Result:** The Published NI Group Assignment tables are listed under the folder in the left pane.

If the folder is empty, add a Published NI Group Assignment table.

**Manage services**

To provision signaling firewall load balancer or distribution function with single IP address exposed for the Gm interface to end users.

To provision a Published NI Group Assignment table

DRAFT

Perform the following steps in the **FEPH Tables** window to add, rename, or delete a Published NI Group Assignment table :

| If you want to ...                            | then ...   |
|---|--|
| add a Published NI Group Assignment table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/> <b>Result:</b> The <b>FEPH Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a Published NI Group Assignment table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/> <b>Result:</b> The <b>FEPH Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |
| delete a Published NI Group Assignment table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Published NI Group Assignment table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>   |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the Published NI Group Assignment table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

DRAFT

- 4 Perform the following steps at the **FEPH Tables** window to add, modify, or delete the Published NI Group Assignment table attributes:

| If you want to ...                                       | then ...  |
|--|---|
| add the Published NI Group Assignment table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>FEPH Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol>   |
| modify a Published NI Group Assignment table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>FEPH Tables</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol> |
| delete a Published NI Group Assignment table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.<br/><i>End of steps</i></li> </ol>            |

**Manage services**

*To provision signaling firewall load balancer or distribution function with single IP address exposed for the Gm interface to end users*

To provision a Published NI Group Assignment table

**5 Provision the following parameters:**

| Parameter                            | Provisioning   |
|--------------------------------------|--|
| <b>Published NI Group Assignment</b> | <p>In the <b>Published NI Group Assignment</b> dialog box that appears, configure the following parameters. This dialog is used to assign service instances (IMS node IDs) to a published NI group.</p> <p>Select the appropriate option from the <b>Service Instance</b> drop-down list. This list defines the Service Instance value (IMS service Node ID – 255) of an IMS service that has a Published NI on the FEPH subnet. The range is 1 to 64.</p> <p><b>Note: Sharing :</b> If the service instance does not exist in any Published NI Group record, it is considered to be NOT SHARED. If the service instance exists in a Published NI Group record, it is considered to be SHARED regardless of whether it is the only service in the group.</p> <p>Remember the following:</p> <ul style="list-style-type: none"> <li>• A service instance can only appear in at most one published NI group.</li> <li>• All service instances within a published NI group must have a Published NI on the FEPH subnet with the same v4/v6 IP address combination.</li> </ul> <p>When a service instance goes from SHARED to NOT-SHARED (delete):</p> <ul style="list-style-type: none"> <li>• If the group has other services assigned to it, then the service instance being deleted must not be FEPH Enabled. If the service being deleted is the only service in the group, then it can be FEPH enabled.</li> <li>• Any P-CSCFs that exist on the affected service(s) who's Port Name matches existing P-CSCFs on non shared IMS services must have the same Permanent Linkset Group Number (in order to confirm to existing rule).</li> </ul> <p>When a service instance goes from NOT-SHARED to SHARED (insert):</p> <ul style="list-style-type: none"> <li>• All PCSCFs in the shared group with the same Port Number must have the same Port Name.</li> <li>• All PCSCFs in the shared group with the same Port Name must have the same ACR Messages Generation, Allow Immediate 200 OK, and Area ID values.</li> </ul> |

*Manage services  
To provision signaling firewall load balancer or distribution function with single IP address exposed for the Gm interface to end users*

To provision a Published NI Group Assignment table

| Parameter                    | Provisioning  |
|------------------------------|---|
| <b>Published NI Group ID</b> | Select the appropriate option from the <b>Published NI Group ID</b> drop-down list.<br><br>This list specifies the ID of the Published NI Group that contains IMS services with the same Published NI v4/v6 combination on the FEPH subnet. The range is 1 to 64. |

For more information on the parameters, see the topic **Published NI Group Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 6 Click OK.

**Result:** The Published NI Group Assignment table attributes are provisioned successfully.

END OF STEPS

# To provision common announcement module (CANM)

## Overview

### Purpose

This section provides the procedures for provisioning the Common Announcement Module (CANM).

### Contents

|   |       |
|---|-------|
| <a href="#">To provision a Treatment Trigger Data Table</a> | 5-236 |
| <a href="#">To provision a CANM Profile Table</a>           | 5-239 |

# To provision a Treatment Trigger Data Table

## Purpose

This procedure is used to provision a Treatment Trigger Data Table.

## Steps to provision a Treatment Trigger Data Table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **CANM Tables**.

**Result:** The **CANM Tables** window is displayed.

- 2 In the left pane, expand the **Treatment Trigger Data** folder.

**Result:** The Treatment Trigger Data tables are listed under the folder in the left pane.

If the folder is empty, add a Treatment Trigger Data Table.

Perform the following steps in the **CANM Tables** window to add, rename, or delete a Treatment Trigger Data Table:

| If you want to ...                     | then ...  |
|--|---|
| add a Treatment Trigger Data Table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>CANM Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a Treatment Trigger Data Table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>CANM Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |

| If you want to ...                     | then ...  |
|--|---|
| delete a Treatment Trigger Data Table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Treatment Trigger Data Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the Treatment Trigger Data Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **CANM Tables** window to add, modify, or delete the Treatment Trigger Data Table attributes:

| If you want to ...                                | then ...   |
|---|--|
| add the Treatment Trigger Data Table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>CANM Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a Treatment Trigger Data Table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>CANM Tables</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                                | then ...  |
|---|---|
| delete a Treatment Trigger Data Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter                                | Provisioning   |
|--|--|
| <b>Treatment Trigger Data Attributes</b> | <p>Configure the following parameters on the <b>Treatment Trigger Data Attributes</b> screen that is displayed.</p> <p>Select the appropriate option from the <b>Treatment ID</b> list.</p> <p>This parameter defines the Treatment Id that will be used in the Treatment Trigger Map data on the CANM Profile.</p> <p><b>Note:</b> A maximum of 10 Treatment Trigger records are allowed to be provisioned.</p> |
| <b>Condition Description</b>             | <p>Enter the appropriate description in the <b>Condition Description</b> field.</p> <p>This parameter describes the condition that the service provider will want to map to an announcement.</p>   |

For more information on the parameters, see the topic **Treatment Trigger Data** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

6 Click **OK**.

**Result:** The Treatment Trigger Data Table attributes are provisioned successfully.

END OF STEPS

# To provision a CANM Profile Table

## Purpose

This procedure is used to provision a CANM Profile Table.

## Steps to provision a CANM Profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **CANM Tables**.

**Result:** The **CANM Tables** window is displayed.

- 2 In the left pane, expand the **CANM Profiles** folder.

**Result:** The CANM Profiles tables are listed under the folder in the left pane.

If the folder is empty, add a CANM Profile table.

Perform the following steps in the **CANM Tables** window to add, rename, or delete a CANM Profile table :

| If you want to ...           | then ...   |
|------------------------------|--|
| add a CANM Profile table,    | <ol style="list-style-type: none"><li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>CANM Tables</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |
| rename a CANM Profile table, | <ol style="list-style-type: none"><li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>CANM Tables</b> window is displayed.</li><li>2. In the <b>Table Name</b> box, type a new table name.</li><li>3. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p>  |

| If you want to ...           | then ...  |
|------------------------------|---|
| delete a CANM Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a CANM Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the CANM Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** **Note:** <notes if any>.

Perform the following steps at the **CANM Tables** window to add, modify, or delete the CANM Profile table attributes:

| If you want to ...                      | then ...  |
|---|---|
| add the CANM Profile table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>CANM Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a CANM Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>CANM Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                      | then ...   |
|---|--|
| delete a CANM Profile table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

**5** Provision the following parameters:

| Parameter                      | Provisioning  |
|--------------------------------|---|
| <b>CANM Profile Attributes</b> | <p>Configure the following parameters on the <b>CANM Profile Attributes</b> screen that is displayed:</p> <p>Select the appropriate CANM Profile ID value from the <b>Profile ID</b> field.</p> <p><b>Note:</b> A maximum of 10 CANM Profile records are allowed to be provisioned. The CANM Profile data is downloaded to the IMS Nodes that have a CANM SIPia port provisioned with the given CANM Profile.</p> |
| <b>Profile Description</b>     | Enter the appropriate description in the <b>Profile Description</b> field.  |

| Parameter                                    | Provisioning  |
|--|---|
| <b>MRF Announcement Interface Profile ID</b> | <p>Select the appropriate value from the <b>MRF Announcement Interface Profile ID</b> drop-down list.</p> <p>The <b>MRF Announcement Interface Profile</b> needs to be provisioned under <b>IMS → Global Tables</b> on the FS GUI. This parameter specifies an instance of the MRF Announcements Interface Profile. If a non-null value is specified, the profile will provide the parameters to include while requesting announcements from the MRF. If this field is null, then no announcements are attempted.</p> <p><b>Note:</b> The <b>MRF Announcement Data</b> table has to be provisioned before provisioning the <b>MRF Announcement Interface Profile</b> profile.</p> |
| <b>Default Language Locale</b>               | <p>Select the appropriate value from the <b>Default Language Locale</b> drop-down list.</p> <p>This parameter provides an indication of the default language/locale to use while sending NetAnn (RFC 4240) formatted announcement requests to the MRF. If per-subscriber locale information is available, then this default locale is not used. If this field is null and there is no per-subscriber locale information, then no locale information is sent to the MRF.</p>   |
| <b>MRF Announcement Guard Timer (secs)</b>   | <p>Enter the appropriate value in the <b>MRF Announcement Guard Timer (secs)</b> field.</p> <p>This parameter specifies the time duration that the CANM will allow an announcement to continue before CANM tears it down. A value of 0 indicates no timer is applied. The default value is 300.</p>   |

| Parameter                               | Provisioning  |
|---|---|
| <b>Provision the Treatment Map Data</b> | <p><b>Provision the Treatment Map Data</b> - Up to 10 Treatment Triggers can be added to the given CANM profile.</p> <p>To add attributes to the Treatment Map Data group box,</p> <ol style="list-style-type: none"> <li>Under the Treatment Map Data group box, click <b>Add</b>.<br/> <b>Result:</b> The <b>Treatment Trigger Mapping</b> screen is displayed.</li> <li>Configure the following parameters <ul style="list-style-type: none"> <li><b>Treatment Id</b> - This parameter provides the mapping data for treatment triggers to announcement data for the MRF.</li> <li><b>Announcement Number</b> - This parameter identifies the index to the announcement number in the MRF Announcements Interface Profile referenced from the CANM Profile. The Announcement Data from the MRF Announcements Interface Profile defines some parameters to be sent to the MRF in the INVITE request.</li> <li><b>Repeat</b> - This parameter denotes the number of times that the announcement should be repeated. This parameter will be sent to the MRF in the INVITE request. A value of 0 means repeat continuously. The default value is 1.</li> <li><b>Delay (msecs)</b> - This parameter denotes the time delay (milliseconds) before playing the announcement. This parameter will be sent to the MRF in the INVITE request.</li> <li><b>Duration (msecs)</b> - This parameter denotes the time duration (milliseconds) to play the announcement (milliseconds). This parameter will be sent to the MRF in the INVITE request. A value of 0 means NO limit.</li> </ul> </li> <li>Click <b>OK</b>.</li> </ol> <p>To modify attributes in the Treatment Map Data group box,</p> <p>Alcatel-Lucent - Proprietary Use pursuant to applicable agreement Under the Treatment Map Data group box, select the row (record) that you wish to modify and click <b>Modify</b>.<br/> <b>Result:</b> The <b>Treatment Trigger Mapping</b> screen is displayed.</p> |

For more information on the parameters, see the topic **CANM Profile** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The CANM Profile table attributes are provisioned successfully.

END OF STEPS

---

# To provision iAGCF support of network traffic management (NTM)

## Overview

### Purpose

This section provides the procedures for provisioning iAGCF support of Network Traffic Management (NTM).

### Contents

|  |       |
|--|-------|
| To provision an AGCF Cause Code To H248 Tone Table | 5-246 |
|--|-------|

# To provision an AGCF Cause Code To H248 Tone Table

## Purpose

This procedure is used to provision an AGCF Cause Code To H248 Tone Table.

## Steps to provision an AGCF Cause Code To H248 Tone table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **AGCF Tables**.

**Result:** The **AGCF Tables** window is displayed.

- 2 In the left pane, expand the **AGCF Cause Code To H248 Tone** folder.

**Result:** The AGCF Cause Code To H248 Tone tables are listed under the folder in the left pane.

If the folder is empty, add an AGCF Cause Code to H248 Tone table.

Perform the following steps in the **AGCF Tables** window to add, rename, or delete an AGCF Cause Code to H248 Tone table :

| If you want to ...                            | then ...  |
|---|---|
| add an AGCF Cause Code to H248 Tone table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>AGCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename an AGCF Cause Code to H248 Tone table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>AGCF Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |

| If you want to ...                            | then ...   |
|---|--|
| delete an AGCF Cause Code to H248 Tone table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an AGCF Cause Code to H248 Tone table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the AGCF Cause Code to H248 Tone table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **AGCF Tables** window to add, modify, or delete the AGCF Cause Code to H248 Tone table attributes:

| If you want to ...                                       | then ...  |
|--|---|
| add the AGCF Cause Code to H248 Tone table attributes,   | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>AGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify an AGCF Cause Code to H248 Tone table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>AGCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                                       | then ...  |
|--|---|
| delete an AGCF Cause Code to H248 Tone table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter                       | Provisioning  |
|---------------------------------|---|
| <b>Cause Code to H.248 Tone</b> | <p>Configure the following parameters on the <b>Cause Code to H.248 Tone</b> screen that is displayed.</p> <p>Select the appropriate option from the <b>Cause Code</b> drop-down list.</p> <p><b>Note:</b> A maximum of 32 records are allowed to be provisioned.</p> |
| <b>H.248 Tone</b>               | Select the appropriate option from the <b>H.248 Tone</b> drop-down list.  |

For more information on the parameters, see the topic **Agcf Variant Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

6 Click **OK**.

**Result:** The AGCF Cause Code to H248 Tone table attributes are provisioned successfully.

END OF STEPS

# To provision CMCC emergency service and P-CSCF SIP header manipulation

## Overview

### Purpose

This section provides the procedures for provisioning CMCC Emergency Service and P-CSCF SIP Header Manipulation.

### Contents

|   |       |
|---|-------|
| To provision an Access Location to ESRN Mapping Table | 5-250 |
| To provision an IP Address Mapping Table              | 5-255 |
| To provision a Default Access Location Table          | 5-259 |

# To provision an Access Location to ESRN Mapping Table

## Purpose

This procedure is used to provision an Access Location to ESRN Mapping Table.

### Before you **delete** an Access Location to ESRN Mapping table

Before you delete an Access Location to ESRN Mapping table, ensure that the table is NOT used by the IP Address Mapping Table or SBC Domain Mapping (Default Access Location) table.

### Steps to provision an Access Location to ESRN Mapping table

Perform the following steps at the Provisioning GUI:

- 1** Select **IMS → IMS Components → ECSCF Tables**.

**Result:** The **ECSCF Tables** window is displayed.

- 2** In the left pane, expand the **Access Location to ESRN Mapping** folder.

**Result:** The Access Location to ESRN Mapping tables are listed under the folder in the left pane.

If the folder is empty, add an Access Location to ESRN Mapping table.

Perform the following steps in the **ECSCF Tables** window to add, rename, or delete an Access Location to ESRN Mapping table :

| If you want to ...                            | then ...  |
|---|---|
| add an Access Location to ESRN Mapping table, | <ol style="list-style-type: none"> <li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>ECSCF Tables</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

*Manage services*

*To provision CMCC emergency service and P-CSCF SIP header manipulation*

To provision an Access Location to ESRN Mapping Table

| If you want to ...                               | then ...  |
|--|---|
| rename an Access Location to ESRN Mapping table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/> <b>Result:</b> The <b>ECSCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>                |
| delete an Access Location to ESRN Mapping table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an Access Location to ESRN Mapping table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the Access Location to ESRN Mapping table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **ECSCF Tables** window to add, modify, or delete the Access Location to ESRN Mapping table attributes:

| If you want to ...  | then ...   |
|---|--|
| add the Access Location to ESRN Mapping table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/> <b>Result:</b> The <b>ECSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...  | then ...   |
|---|--|
| modify an Access Location to ESRN Mapping table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>ECSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete an Access Location to ESRN Mapping table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                |

**5** Provision the following parameters:

| Parameter                 | Provisioning   |
|---------------------------|--|
| <b>Access Location ID</b> | Enter the appropriate value in the <b>Access Location ID</b> field.<br><b>Note:</b> A maximum of 200 records are allowed to be provisioned.                            |
| <b>Access Location</b>    | Enter the appropriate value in the <b>Access Location</b> field.<br>The maximum number of allowed characters is 75 and the allowed values are A-Z, a-z, space and “-”. |

*Manage services*

*To provision CMCC emergency service and P-CSCF SIP header manipulation*

To provision an Access Location to ESRN Mapping Table

| Parameter                             | Provisioning   |
|---------------------------------------|--|
| <b>Emergency ID to Routing Number</b> | <p>Provision the <b>Emergency ID to Routing Number</b> group box.</p> <p>To add attributes to the <b>Emergency ID to Routing Number</b> group box,</p> <ol style="list-style-type: none"> <li>Under the <b>Emergency ID to Routing Number</b> group box, click <b>Add</b>.<br/> <b>Result:</b> The <b>Add/Modify Emergency ID to Routing Number</b> screen is displayed.</li> <li>Configure the following parameters <ul style="list-style-type: none"> <li>Enter the appropriate value in the <b>Emergency Identifier</b> field.<br/> This field contains one among the 10 emergency identifiers for the specified access location.<br/> Each emergency ID is found at <b>IMS</b> → <b>IMS tables</b> → <b>IMS</b> → <b>General</b> → <b>Emergency Identifiers list</b>.</li> <li>Enter the appropriate value in the <b>PSAP Routing Number</b> field.<br/> This field specifies the PSAP Routing Number for the Access Location and Emergency Identifier specified. Each PSAP routing number is a global E.164 number ('+' sign followed by an international telephone number).</li> </ul> </li> </ol> <p><b>Note :</b> The <b>Access Location</b> field will be grayed out as it will be populated with the Access Location from the previous screen and cannot be changed here.</p> <ol style="list-style-type: none"> <li>Click <b>OK</b>.</li> </ol> <p>To modify attributes in the <b>Emergency ID to Routing Number</b> group box,</p> <ol style="list-style-type: none"> <li>Under the <b>Emergency ID to Routing Number</b> group box, select the record that you wish to modify and click <b>Modify</b>. Alternatively, select the record that you wish to modify and double-click.<br/> <b>Result:</b> The <b>Add/Modify Emergency ID to Routing Number</b> screen is displayed.</li> <li>Modify the desired parameters and click <b>OK</b>.</li> </ol> <p>To delete attributes in <b>Emergency ID to Routing Number</b> group box,</p> <ol style="list-style-type: none"> <li>Under the <b>Emergency ID to Routing Number</b> group box, select the record that you wish to delete and click <b>Delete</b>.</li> <li>Click <b>OK</b> to confirm.</li> </ol> |

For more information on the parameters, see the topic **Access Location to ESRN Mapping Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The Access Location to ESRN Mapping table attributes are provisioned successfully.

---

END OF STEPS

---

# To provision an IP Address Mapping Table

## Purpose

This procedure is used to provision an IP Address Mapping Table.

## Before you begin

**Note:** The Access Location table must be provisioned before provisioning the IP Address Mapping Table.

## Steps to provision an IP Address Mapping Table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → ECSCF Tables**.

**Result:** The **ECSCF Tables** window is displayed.

- 2 In the left pane, expand the **IP Address Mapping** folder.

**Result:** The IP Address Mapping tables are listed under the folder in the left pane.

If the folder is empty, add an IP Address Mapping Table.

Perform the following steps in the **ECSCF Tables** window to add, rename, or delete an IP Address Mapping Table :

| If you want to ...               | then ...  |
|----------------------------------|---|
| add an IP Address Mapping Table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>ECSCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                  | then ...   |
|-------------------------------------|--|
| rename an IP Address Mapping Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>ECSCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>    |
| delete an IP Address Mapping Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an IP Address Mapping Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the IP Address Mapping Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **ECSCF Tables** window to add, modify, or delete the IP Address Mapping Table attributes:

| If you want to ...                           | then ...  |
|--|---|
| add the IP Address Mapping Table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>ECSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                             | then ...   |
|--|--|
| modify an IP Address Mapping Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>ECSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete an IP Address Mapping Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                |

**5** Provision the following parameters:

| Parameter             | Provisioning  |
|-----------------------|---|
| <b>IP Range ID</b>    | Enter the appropriate value in the <b>IP Range ID</b> field.<br><b>Note:</b> A maximum of 20,000 records are allowed to be provisioned. |
| <b>IP Range Start</b> | Enter the appropriate value in the <b>IP Range Start</b> field.<br>This field denotes the V4 or V6 IP address to begin the range.       |

| Parameter       | Provisioning  |
|-----------------|---|
| IP Range End    | <p>Enter the appropriate value in the <b>IP Range End</b> field.</p> <p>This field denotes the V4 or V6 IP address to end the range. The format of this IP address must match the format of the IP Start Range address. The IP Range End address of one IP range should be greater than or equal to its IP Range Start address.</p> <p><b>Note :</b> If one IP range overlaps with the other IP range, the GUI will not detect this error. The administrator should ensure that one IP range in the IP Address Mapping Table does not overlap with another.</p> |
| Access Location | <p>Select the appropriate value from the <b>Access Location</b> list.</p> <p>This field specifies the Access Location for this IP range. This list contains the Access Location values defined in the <b>Access Location</b> table.</p>   |

For more information on the parameters, see the topic **IP Address Mapping Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

6 Click OK.

**Result:** The IP Address Mapping Table attributes are provisioned successfully.

END OF STEPS

# To provision a Default Access Location Table

## Purpose

This procedure is used to provision a Default Access Location Table.

## Before you begin

**Note:** The Access Location table must be provisioned before provisioning the Default Access Location Table.

## Steps to provision a Default Access Location Table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → ECSCF Tables**.

**Result:** The **ECSCF Tables** window is displayed.

- 2 In the left pane, expand the **Default Access Location** folder.

**Result:** The Default Access Location tables are listed under the folder in the left pane.

If the folder is empty, add a Default Access Location Table.

Perform the following steps in the **ECSCF Tables** window to add, rename, or delete a Default Access Location Table :

| If you want to ...                   | then ...  |
|--------------------------------------|---|
| add a Default Access Location Table, | <ol style="list-style-type: none"><li>Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>ECSCF Tables</b> window is displayed.</li><li>From the <b>Table Number</b> list, select the table number.</li><li>In the <b>Table Name</b> box, type a descriptive table name.</li><li>Click <b>OK</b>.<br/><i>End of steps</i></li></ol> |

| If you want to ...                      | then ...   |
|---|--|
| rename a Default Access Location Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>ECSCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>        |
| delete a Default Access Location Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Default Access Location Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the Default Access Location Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **ECSCF Tables** window to add, modify, or delete the Default Access Location Table attributes:

| If you want to ...                                | then ...  |
|---|---|
| add the Default Access Location Table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>ECSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                                 | then ...   |
|--|--|
| modify a Default Access Location Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>ECSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a Default Access Location Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                |

**5** Provision the following parameters:

| Parameter              | Provisioning   |
|------------------------|--|
| <b>Domain ID</b>       | Enter the appropriate value in the <b>Domain ID</b> field.<br><br><b>Note:</b> A maximum of 256 records are allowed to be provisioned.   |
| <b>Domain</b>          | Enter the appropriate value in the <b>Domain</b> field.<br><br>A maximum of 100 characters are allowed and the allowed characters are 0-9, a-z, A-Z, “.” and “-”.  |
| <b>Access Location</b> | Select the appropriate value from the <b>Access Location</b> drop-down list.<br><br>This field specifies the Access Location for this SBC domain. This drop-down list contains the Access Location values defined in the <b>Access Location</b> table. |

For more information on the parameters, see the topic **SBC Domain Mapping Table (Default Access Location)** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The Default Access Location Table attributes are provisioned successfully.

---

END OF STEPS

---

# To provision support for sending offline charging data to the CCF provisioned to the CTS

## Overview

### Purpose

This section provides a brief description of the provisioning procedure to be followed to support sending offline charging data to the CCF provisioned to the CTS.

### Contents

|   |       |
|---|-------|
| Support sending offline charging data to the CCF provisioned to the CTS | 5-264 |
|---|-------|

# Support sending offline charging data to the CCF provisioned to the CTS

## Overview

The feature “Support sending offline charging data to the CCF provisioned to the CTS” provides the following functionalities to ensure that the offline charging data can be sent to the specified CCF provided in the HSS per UE:

- Support M.D configuration including switch between G.R and M.D.

### Warning!

1. Do not perform the switch operation during high ACR traffic in order to avoid sending of the ACRs to unexpected CCFs
  2. Do not perform the switch operation in little or none ACR traffic window
  3. When performing the switch operation from G.R. to M.D., add a Primary or Secondary FQDN with the **Backup FQDN** field selected
  4. Switch operation from M.D. to G.R. is not recommended
- Support to get CCF address from the HSS, to update them in time and to insert CCF address into SIP message per session.

**Note:** G.R and M.D are exclusive configurations. That is, for the same service, it can only use one kind of configuration, G.R or M.D, but not both.

This feature introduces the following options on the FS GUI:

- **Pass HSS Provided CCF address** - This option is added in the S-CSCF profile to indicate whether to insert the CCF address received from the HSS in the SIP message.
- **Use HSS Provided CCF address** - This option is added in the ACR charging profile to indicate whether to use the CCF address provided in the HSS.

If both the options above are checked, then the Application (CTS) sends the CCF address provided in the HSS to the Rf interface, and all the charging information in this session will be sent to the specified CCF if the diameter configuration of this application is M.D. Rf interface will not use CCF addresses passed by the application if the diameter configuration is G.R.

For detailed information on the provisioning task flow, see “[Support sending offline charging data to the CCF provisioned to the CTS - Provisioning task flow](#)” (p. 1-80).

# To provision limit for TCP connections

## Overview

### Purpose

This section describes the procedures for provisioning limit for TCP connections.

### Contents

|                                       |       |
|---------------------------------------|-------|
| To provision a Remote IP Policy Table | 5-266 |
|---------------------------------------|-------|

# To provision a Remote IP Policy Table

## Purpose

This procedure is used to add, modify, or delete a Remote IP Policy Table.

## Steps to provision a Remote IP Policy Table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → FEPH Tables**.

**Result:** The **FEPH Tables** window is displayed.

- 2 In the left pane, expand the **Remote IP Policy** folder.

**Result:** The Remote IP Policy tables are listed under the folder in the left pane.

If the folder is empty, add a Remote IP Policy Table.

Perform the following steps in the **FEPH Tables** window to add, rename, or delete a Remote IP Policy Table :

| If you want to ...               | then ...   |
|----------------------------------|--|
| add a Remote IP Policy Table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>FEPH Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a Remote IP Policy Table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>FEPH Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |

| If you want to ...               | then ...   |
|----------------------------------|--|
| delete a Remote IP Policy Table, | <ol style="list-style-type: none"><li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li><li>2. Click <b>Yes</b> to confirm deletion</li></ol> <p><b>Note:</b> Before you delete a Remote IP Policy Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the Remote IP Policy Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **FEPH Tables** window to add, modify, or delete the Remote IP Policy Table attributes:

| If you want to ...                          | then ...   |
|---|--|
| add the Remote IP Policy Table attributes,  | <ol style="list-style-type: none"><li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>FEPH Tables</b> window is displayed.</li><li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li></ol> <p><i>End of steps</i></p>  |
| modify a Remote IP Policy Table attributes, | <ol style="list-style-type: none"><li>1. In the right pane, select the profile that you want to modify.</li><li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>FEPH Tables</b> window is displayed.</li><li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li></ol> <p><i>End of steps</i></p> |

| If you want to ...                          | then ...  |
|---|---|
| delete a Remote IP Policy Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter                        | Provisioning   |
|----------------------------------|--|
| <b>Policy Id</b>                 | Select the appropriate option from the <b>Policy Id</b> field.<br><br>This parameter identifies the instance of the Remote IP Policy. The default value is 1.  |
| <b>Description</b>               | Enter the description in the <b>Description</b> field.   |
| <b>Maximum Inbound TCP Flows</b> | Select the appropriate value from the <b>Maximum Inbound TCP Flows</b> list.<br><br>This parameter specifies the total number of inbound initiated TCP flows that are allowed for the Remote IP to which the policy is assigned.<br><br>The default value (65535) is “no limit”. The value 65,535 is the theoretical maximum for flows that could be distinguished. Using that value is essentially a “no limit”. The value “0” means “drop all”.<br><br>Due to the need to establish new TCP flows after a BEPH switch over, and the lag in deleting the previous flows, this number should typically be set to double the expected usage of a remote IP. |

| Parameter                                   | Provisioning   |
|---|--|
| <b>Affinity flow Threshold Match String</b> | <p>Enter an appropriate value in the <b>Affinity flow Threshold Match String</b> field.</p> <p>This field specifies the maximum number of concurrent flows for the Remote IP that can be in progress and still have the preferred BEPH instance to be considered for flow distribution.</p> <p>The default value is 10. If the number of flows is <math>\leq</math> this threshold, then the preferred BEPH instance in the Remote IP table is considered while distributing a new inbound-initiated flow for that remote IP address. If the number of flows is <math>&gt;</math> this threshold, then the preferred BEPH instance is not considered. "0" mean no affinity.</p> <p>See also, "<a href="#">To provision signaling firewall load balancer or distribution function with single IP address exposed for the Gm interface to end users</a>" (p. 5-229).</p> |

For more information on the parameters, see the topic **Feph Remote Ip Policy Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 6 Click **OK**.

**Result:** The Remote IP Policy Table attributes are provisioned successfully.

END OF STEPS

# To provision IMUX services

## Overview

### Purpose

This section describes the provisioning procedures to facilitate IMUX services.

### Contents

|  |       |
|--|-------|
| To provision IMUX to IMS Association Table | 5-271 |
| To provision IMUX port                     | 5-274 |

# To provision IMUX to IMS Association Table

## Overview

This procedure is used to provision IMUX to IMS Association table.

## Steps to provision IMUX to IMS Association Table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMUX Tables**.

**Result:** The **IMUX Tables** window is displayed.

- 2 In the left pane, expand the **IMUX to IMS Association** folder.

**Result:** The IMUX to IMS Association tables are listed under the folder in the left pane.

If the folder is empty, add IMUX to IMS Association Table.

Perform the following steps in the **IMUX Tables** window to add, rename, or delete IMUX to IMS Association Table :

| If you want to ...                    | then ...  |
|---------------------------------------|---|
| add IMUX to IMS Association Table,    | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>IMUX Tables</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |
| rename IMUX to IMS Association Table, | <ol style="list-style-type: none"><li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>IMUX Tables</b> window is displayed.</li><li>2. In the <b>Table Name</b> box, type a new table name.</li><li>3. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p>  |

| If you want to ...                    | then ...   |
|---------------------------------------|--|
| delete IMUX to IMS Association Table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete IMUX to IMS Association Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the IMUX to IMS Association Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **IMUX Tables** window to add, modify, or delete the IMUX to IMS Association Table attributes:

| If you want to ...                                | then ...   |
|---|--|
| add the IMUX to IMS Association Table attributes, | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>IMUX Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify IMUX to IMS Association Table attributes,  | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>IMUX Tables</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                               | then ...  |
|--|---|
| delete IMUX to IMS Association Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter                       | Provisioning   |
|---------------------------------|--|
| <b>IMUX Cluster ID</b>          | The <b>IMUX Cluster ID</b> is a drop-down list that contains IMUX pool IDs. This parameter is unavailable for editing.   |
| <b>IMS Node ID</b>              | The <b>IMS Node ID</b> is a drop-down list which contains all the node IDs that have a default NI with the same v4 or v6 IP address combination as the IMUX currently selected. This parameter is unavailable for editing. |
| <b>Default NI v4 IP address</b> | The <b>Default NI v4 IP address</b> parameter displays the shared IMS/IMUX default NI v4 IP address  |
| <b>Default NI v6 IP address</b> | The <b>Default NI v6 IP address</b> parameter displays the shared IMS/IMUX default NI v6 IP address  |

For more information on the parameters, see the topic **Imux To Ims Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

6 Click **OK**.

**Result:** The IMUX to IMS Association Table attributes are provisioned successfully.

END OF STEPS

# To provision IMUX port

## Overview

This procedure is used to provision IMUX Port. IMUX Port represents a set of SIPia ports on the IMS services that share the IP with the IMUX service.

## Before you begin

The corresponding IMS SIPia ports must be created before the IMUX ports are created.

### Warning!

IMUX Port operations may affect operation of IMS SIPia ports, so it is recommended to perform operations during maintenance intervals while IMS ports are locked.

## Steps to provision IMUX Port Table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMUX Tables**.

**Result:** The **IMUX Tables** window is displayed.

- 2 In the left pane, expand the **IMUX Port** folder.

**Result:** The IMUX Port Tables are listed under the folder in the left pane.

If the folder is empty, add IMUX Port Table.

Perform the following steps in the **IMUX Tables** window to add, rename, or delete IMUX Port Table :

| If you want to ...   | then ...   |
|----------------------|--|
| add IMUX Port Table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>IMUX Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...      | then ...  |
|-------------------------|---|
| rename IMUX Port Table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>IMUX Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete IMUX Port Table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete IMUX Port Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>            |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the IMUX Port Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **IMUX Tables** window to add, modify, or delete the IMUX Port Table attributes:

| If you want to ...                  | then ...   |
|-------------------------------------|--|
| add the IMUX Port Table attributes, | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>IMUX Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                 | then ...  |
|------------------------------------|---|
| modify IMUX Port Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>IMUX Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete IMUX Port Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>           |

**5** Provision the following parameters:

| Parameter              | Provisioning   |
|------------------------|--|
| <b>IMUX Cluster ID</b> | The <b>IMUX Cluster ID</b> is a drop-down list that contains IMUX pool IDs. This parameter is unavailable for editing. |

| Parameter          | Provisioning  |
|--------------------|---|
| <b>Port Type</b>   | <p>The <b>Port Type</b> parameter identifies one of the SIPia Port Types that are configured within the cluster.</p> <p>The <b>Port Type</b> drop-down list can contain the following options that are derived from this cluster:</p> <ul style="list-style-type: none"> <li>• ICSF PORT</li> <li>• SCSF PORT</li> <li>• BGCF PORT</li> <li>• ECSF PORT</li> <li>• LIF PORT</li> </ul> <p><b>Note:</b> LIF Ports behaves the same as SIPia LIF ports. To provision this, the user must have surveillance role.</p> <p>This parameter is unavailable for provisioning.</p> |
| <b>Port Name</b>   | <p>The <b>Port Name</b> parameter identifies one of the GULs that are configured within the cluster.</p> <p>This drop-down list contains the SIPia port names associated to the selected Port Type that exist on the IMS nodes contained in the selected IMUX cluster.</p> <p>This field is unavailable for provisioning.</p> <p>This window is unavailable if no SIPia ports exist in the IMS nodes in the selected IMUX cluster.</p>  |
| <b>Port Number</b> | <p>In the <b>Port Number</b> box, enter the port number used by IMUX.</p> <p>The available range is 1 to 32767. The default and recommended port number is 5060. Also, note that the selected port number must be different from the port numbers used by IMS services in the cluster. The port must be the same if the GUL is same on the other IMUX.</p>  |

| Parameter                         | Provisioning  |
|-----------------------------------|---|
| <b>Administrative State</b>       | <p>From the <b>Administrative State</b> drop-down list, select <b>Lock</b> to lock the IMUX port, and <b>Unlock</b> to unlock the IMUX port. The default value is Lock.</p> <p>This parameter identifies if the IMUX port is in locked or unlocked state.</p> <p><b>Note:</b> IMUX is configured in the Locked state. When you want to bring IMS or IMUX ports into service, you must bring the IMS ports into service first and then bring the IMUX ports into service.</p> <p>When you want to lock an IMS port in the system, you must lock the ports on every IMS service first, before you lock the IMUX ports. Locking IMUX first disrupts communication to the active IMS ports.</p> |
| <b>Overload Special Treatment</b> | <p>From the <b>Overload Special Treatment</b> drop-down list, select one of the following options:</p> <ul style="list-style-type: none"> <li>• Reject with 500</li> <li>• Pass Through</li> </ul> <p>This treatment is for IMUX behavior when it is in MAJOR overload. The default setting is Reject with 500. When it is in CRITICAL overload, IMUX shall reject with 500.</p> <p>On inserts, the value is forced to match the value of the SIPia port. On updates, the change is applied to all SIPia and IMUX ports with the same port name.</p>  |

For more information on the parameters, see the topic **IMUX Port Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

6 Click OK.

**Result:** The IMUX Port Table attributes are provisioned successfully.

END OF STEPS

# To provision iHSS/iSLF support of per-enterprise domains

## Overview

### Purpose

This section describes the iHSS/iSLF support of per-enterprise domains and the provisioning procedure for the Subscriber Home Domain table.

### Contents

|   |                       |
|---|-----------------------|
| <a href="#">iHSS/iSLF support of per-enterprise domains</a>   | <a href="#">5-280</a> |
| <a href="#">Provisioning the Subscriber Home Domain Table</a> | <a href="#">5-281</a> |

# iHSS/iSLF support of per-enterprise domains

## Overview

The feature “**iHSS/iSLF support of per-enterprise domains**” allows enterprise customers to provision their own domain while adding subscribers.

## Descriptions

Prior to this, the iHSS/iSLF only supported single home domain which is the NGSS default home domain. PRIDs/PUIDs were either domainless or belonged to the default home domain. When there was a need to support multiple enterprise customers, the user identities needed to be made up with the domain of the enterprise, such as dn1@enterprise1.com, dn2@enterprise2.com and so on. Registration using these user identifiers was not possible due to the iHSS limitation.

A per-LCP basis Subscriber Home Domain table was made available so that when operators added user identities, they could select the domain to which each user identity belongs. A maximum of 2048 domains were supported to match with the CSCF home domain entry limit. For the purpose of making iHSS/iSLF able to handle multiple home domains for all user identities (PRIDs and PUIDs) while sending or receiving Cx/Dx/Sh/Dh messages, a table was provided that defines the home domains included in the home network of the operator. This table is provisioned through the OMC-P.

Private IDs can now either be domainless or can be associated with any provisioned home domain. A PUID can either be TEL (in which case it is domainless) or SIP (must be associated with a provisioned home domain). Wildcard PUIDs are inherently domainless.

Prior to implementation of this feature, the iHSS tolerated cases where a CPE registered using a domainless PRID (“abc”) even though the PRID was not provisioned as domainless in the iHSS database. An assert was fired to call attention to this inconsistency between CPE and iHSS provisioning, but the registration was allowed to succeed. However, once multiple PRID domains are supported, “abc” and “abc@domain” could actually be different valid PRIDs. Due to this ambiguity, the iHSS must rely on provisioned data, and can no longer assume a particular domain for a PRID like “abc”. Therefore it is necessary to ensure that CPE and iHSS PRID provisioning is consistent prior to upgrading to the release that includes this feature.

See “[Provisioning the Subscriber Home Domain Table](#)” (p. 5-281) for more information.

# Provisioning the Subscriber Home Domain Table

## Purpose

This procedure is used to provision the Subscriber Home Domain Table.

## Before you begin

### Points to remember

- The number of tables allowed is one per LCP. The maximum number of records that can be provisioned per table is 2048. The Domain Index range is 1 to 2048.
- The association between a domain index and a domain name is not changed without deleting the index domain pair.
- The Domain Name cannot be modified after provisioning. The Domain Name cannot be same (case insensitive) across different records.
- After SU (Software Update) of the system is completed, the per-LCP basis Subscriber Home Domain Table is created with the NGSS Parameter “Default Home Domain” being added as one record of the table.
- Deletion of records is allowed but a warning message pops up when you try to delete records on the GUI screen.
- OMC-P fully supports the domain provisioning.

## Procedure

Perform the following steps at the Provisioning GUI.

- 
- 1 Navigate to **IMS > Global Tables**.

**Result:** The **Global Tables** window is displayed.

---

- 2 Expand the **Subscriber Home Domain** folder, or click **Subscriber Home Domain** if the folder is empty.

3

| If you want to.. | then...  |
|------------------|--|
| add a table,     | <ol style="list-style-type: none"> <li>Right-click <b>Subscriber Home Domain</b> and select <b>Add Table</b> from the menu. <b>Note :</b> A maximum of 1 table of this type is allowed.</li> <li>Select the Table number from the <b>Table number</b> field.</li> <li>Type a unique (descriptive) name in the <b>Table name</b> field.</li> <li>Click <b>OK</b>.</li> </ol> <p><b>Result:</b> A new Subscriber Home Domain table is added.</p> <p><i>End of steps.</i></p> |
| rename a table,  | <p>Select the table that you want to rename.</p> <ol style="list-style-type: none"> <li>Right-click the table and select <b>Rename Table</b> from the menu.</li> <li>Rename the table.</li> <li>Click <b>OK</b> to confirm.</li> </ol> <p><i>End of steps.</i></p>   |
| delete a table,  | <p>Select the table that you want to delete.</p> <ol style="list-style-type: none"> <li>Right-click the table and select <b>Delete Table</b> from the menu.</li> <li>Click <b>OK</b> to confirm.</li> </ol> <p><i>End of steps.</i></p>  |

E N D O F S T E P S

## Subscriber Home Domain Table provisioning procedure

Perform the following steps at the Provisioning GUI.

- 1 Navigate to **IMS > Global Tables**.

**Result:** The **Global Tables** window is displayed.

- 2 Expand the **Subscriber Home Domain** folder.

- 3 To open the table, right-click the desired entry and select **Open** from the menu.

**Result:** The table populates.

4

| If you want to...        | then...  |
|--------------------------|--|
| add table attributes,    | Right-click in the right pane and select <b>Add Table Attributes</b> and proceed with Step 5.  |
| delete table attributes, | <p>Perform the following steps.</p> <ol style="list-style-type: none"> <li>1. Select <b>Delete Table Attributes</b>.<br/> <b>Note:</b> Do not delete the table attributes if the table it is assigned to any user identities in the network.</li> <li>2. Click <b>Yes</b> to confirm.</li> </ol> |

- 5 In the **Subscriber Home Domain** window, select the appropriate value from the **Domain Index** list.

This field specifies the index of the domain, selected by the provisioner to simplify geo redundancy procedures (for example, peer sync). The value “0” is reserved for domainless user identities (PRIDs and PUIDs).

- 6 In the **Domain Name** field, enter the name of the domain in the operator’s home network, that can be assigned to user identities (including PRSET private user identities) when they are added or updated. Sub-domains are allowed.

The format followed is RFC3261 definition for “hostname”. Value 219 is arrived at by taking the maximum length of a PUID supported by Billing which is 256 and subtracting 4 characters for the scheme, 1 characters for the ‘@’ delimiter and 32 characters for the existing PUID Username field.

The Domain Name is unique within the Subscriber Home Domain Table. The maximum character length of the Domain Name field is 219.

The domain name is obtained as follows:

- If the Default Home Domain in NGSS Parameters is populated and the length of Default Home Domain does not exceed 219 characters, then the Default Home Domain is assigned as the Subscriber Home Domain Name in the record.
- Else, the Host Name in NGSS Parameters is assigned as the Subscriber Home Domain Name in the record.

- 
- 7 Click OK.

**Result:** The Subscriber Home Domain table attributes are provisioned successfully.

For more information , see the *Alcatel-Lucent Control Platform 1800/1000/5400 Configuration Database Interface Specification and Object Descriptions Manual*,  
275-900-379

END OF STEPS

---

# To provision MSRP peak data rate support to enhance user experience

## Overview

### Purpose

This section provides the procedure for provisioning MSRP Peak Data Rate to enhance user experience.

### Contents

|  |       |
|--|-------|
| <a href="#">To provision an SDP Media MSRP Table</a> | 5-286 |
|--|-------|

# To provision an SDP Media MSRP Table

## Purpose

This procedure is used to provision an SDP Media MSRP Table.

## Steps to provision an SDP Media MSRP Table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → SCSCF Tables**.

**Result:** The **SCSCF Tables** window is displayed.

- 2 In the left pane, expand the **SDP Media MSRP** folder.

**Result:** The SDP Media MSRP tables are listed under the folder in the left pane.

If the folder is empty, add an SDP Media MSRP Table.

Perform the following steps in the **SCSCF Tables** window to add, rename, or delete an SDP Media MSRP Table :

| If you want to ...              | then ...  |
|---------------------------------|---|
| add an SDP Media MSRP Table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>SCSCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename an SDP Media MSRP Table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables → Rename table</b>.<br/><b>Result:</b> The <b>SCSCF Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |

| If you want to ...              | then ...   |
|---------------------------------|--|
| delete an SDP Media MSRP Table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an SDP Media MSRP Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the SDP Media MSRP Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **SCSCF Tables** window to add, modify, or delete the SDP Media MSRP Table attributes:

| If you want to ...                         | then ...  |
|--|---|
| add the SDP Media MSRP Table attributes,   | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SCSCF Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify an SDP Media MSRP Table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SCSCF Tables</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                         | then ...  |
|--|---|
| delete an SDP Media MSRP Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

---

**5** Provision the following parameters:

| Parameter         | Provisioning   |
|-------------------|--|
| <b>ID</b>         | From the <b>ID</b> list, select the MSRP record ID.          |
| <b>Media Type</b> | From the <b>Media Type</b> list, select the MSRP media type. |
|                   |  |

For more information on the parameters, see the topic **SDP Media MSRP** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

---

**6** Click **OK**.

**Result:** The SDP Media MSRP Table attributes are provisioned successfully.

END OF STEPS

---

# To provision access border for IMS or pre-IMS core

## Overview

### Purpose

This section describes the provisioning procedures for the IBC Access Border for pre-IMS Core domains.

### Contents

|                                 |       |
|---------------------------------|-------|
| To provision IBC-A Profile      | 5-290 |
| To provision IBC Route Profile  | 5-297 |
| To provision Target Group Table | 5-304 |
| To provision Target Group List  | 5-310 |
| To provision IBC Domain Table   | 5-314 |
| To provision Trunk Group        | 5-318 |
| To provision ACL List           | 5-322 |

# To provision IBC-A Profile

## Purpose

This procedure describes the steps to provision IBC-A Profile.

## Before you begin

### Note:

- Only one IBC-A Profile Table can be provisioned.
- Maximum 1024 IBC-A Profile records can be provisioned.

## Steps to provision an IBC-A Profile Table

Perform the following steps at the Provisioning GUI:

- 1** Select **IMS** → **IMS Components** → **PCSCF Tables**.

**Result:** The **PCSCF Tables** window is displayed.

- 2** In the left pane, expand the **IBC-A Profile** folder.

**Result:** The IBC-A Profile Tables are listed under the folder in the left pane.

If the folder is empty, add an IBC-A Profile Table.

Perform the following steps in the **PCSCF Tables** window to add, rename, or delete an IBC-A Profile Table :

| If you want to ...          | then ...   |
|-----------------------------|--|
| add an IBC-A Profile Table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...             | then ...  |
|--------------------------------|---|
| rename an IBC-A Profile Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete an IBC-A Profile Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an IBC-A Profile Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>   |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the IBC-A Profile Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **PCSCF Tables** window to add, modify, or delete the IBC-A Profile Table attributes:

| If you want to ...                      | then ...  |
|---|---|
| add the IBC-A Profile Table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                        | then ...   |
|---|--|
| modify an IBC-A Profile Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete an IBC-A Profile Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                |

**5** Provision the following parameters:

| Parameter                          | Provisioning   |
|------------------------------------|--|
| <b>Profile Id</b>                  | In the <b>Profile Id</b> field, select a profile ID.   |
| <b>Description</b>                 | In the <b>Description</b> field, enter a brief description up to 15 characters.  |
| <b>SIP Filter Set Towards Core</b> | <p>In the <b>SIP Filter Set Towards Core</b> list, select the SIP Filter Set Id that you want to associate to this profile. By default, it is None.</p> <p>Select the following check boxes as applicable for this profile:</p> <ul style="list-style-type: none"> <li>• Apply Privacy</li> <li>• Support 3xx</li> <li>• Disable 3GPP headers</li> <li>• Provide P-CSCF IP address to Core</li> <li>• Use Registry Cache Data</li> <li>• Insert ue-addr</li> </ul> |

| Parameter                                 | Provisioning   |
|---|--|
| <b>IP Version to Provide to Access</b>    | <p>From the <b>IP Version to Provide to Access</b> list, select the IPv4 or IPv6.</p> <p>This field determines whether to include IPv4 or IPv6 version in the Contact header of requests sent to the access network when P-CSCF has both. If P-CSCF is only provisioned with one IP version for the interface to the access network, then this field is ignored.</p>                     |
| <b>IP Version to Provide to Core</b>      | <p>From the <b>IP Version to Provide to Core</b> list, select the IPv4 or IPv6. The default value is IPv4.</p> <p>When “Provide P-CSCF IP Address to Core” is set to ‘Yes’, this field determines whether to include IPv4 or IPv6 version when P-CSCF has both. If P-CSCF is only provisioned with one IP version for the interface to the core, then this field is ignored.</p>         |
| <b>Maximum number of redirects</b>        | <p>From the <b>Maximum number of redirects</b> list, select the value in the range of 1 to 10 and the default is 10.</p>   |
| <b>Permanently Quarantined Users List</b> | <p>From the <b>Permanently Quarantined Users List</b> list, select the ACL List.</p> <p>This field specifies a pointer to an ACL List table, where the content of the list specifies a list of users that are always blocked from sending any SIP messages.</p> <p><b>Note:</b> The ACL pointer provisioned here must not appear in Permanently Trusted Non-Registering Users field.</p> |

| Parameter    | Provisioning  |
|--------------|---|
| Registration | <p>Under the <b>Registration</b> group,</p> <ul style="list-style-type: none"> <li>• Select the following check boxes as applicable:           <ul style="list-style-type: none"> <li>– Contact Rewrite</li> <li>– Service Route Not Required</li> <li>– Path Header Not Included</li> <li>– Don't subscribe to 'reg' Event</li> <li>– P-Associated-URI not required</li> <li>– Use Derived Private ID</li> </ul> </li> <li>• The <b>Access Next Hop</b> list displays the IBC Route profile IDs and is unavailable now. It will be activated in the future releases.</li> <li>• From the <b>Core Next Hop</b> list, select the IBC Route profile IDs.</li> </ul> <p><b>Note:</b></p> <p>Cross Verification</p> <ul style="list-style-type: none"> <li>• Core Next Hop for Registration must point to a valid IBC Route Profile if non-zero.</li> <li>• If the IBC-A Profile is used by a PCSCF Profile with IBC Access Mode set to Non-3GPP IBC or 3GPP P-CSCF, the following fields should have fixed value: Contact Rewrite – No; Path Header Not Included – No; Don't Subscriber to 'reg' Event – No; Service Route Not Required – No; P-Associated-URI Not Required – No; Use Derived Private-ID – No; Disable 3GPP Headers - No; Insert ue-addr - No</li> </ul> |

| Parameter        | Provisioning  |
|------------------|---|
| Non-Registration | <p>Under the <b>Non-Registration</b> group,</p> <ul style="list-style-type: none"> <li>From the <b>Access Next Hop</b> list, select the appropriate value.</li> <li>From the <b>Core Next Hop</b> list, select the appropriate value.</li> <li>From the <b>Allow Unregistered Originations</b> list, select the appropriate option.<br/>The available options:           <ul style="list-style-type: none"> <li>All</li> <li>Emergency Only</li> <li>ACL List Only</li> <li>No</li> </ul>           The default value is Emergency Only.         </li> <li>From the <b>Permanently Trusted Non-Registering Users List</b> list, select the appropriate ACL List ID.</li> </ul> <p><b>Note:</b></p> <p>Cross-Check Verification</p> <ul style="list-style-type: none"> <li>If Allow Unregistered Originations is set to ACL List Only, then Permanently Trusted Non-Registering Users List must point to a valid ACL List.</li> <li>Permanently Trusted Non-Registering Users List and Permanently Quarantine Users List cannot point to the same ACL List.</li> <li>Permanently Trusted Non-Registering Users List must point to a valid ACL List if non-zero.</li> <li>Access Next Hop for Non-Registration must point to a valid IBC Route Profile if non-zero.</li> <li>Core Next Hop for Non-Registration must point to a valid IBC Route Profile if non-zero.</li> </ul> |

For more information on the parameters, see the topic **IBC-A Profile Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The IBC-A Profile Table attributes are provisioned successfully.

END OF STEPS

---

# To provision IBC Route Profile

## Purpose

This procedure describes the steps to provision IBC Route profile.

## Before you begin

### Note:

- Only one IBC Route Profile Table can be provisioned.
- Maximum 1024 IBC Route Profile records can be provisioned.

## Steps to provision a IBC Route Profile Table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → PCSCF Tables**.

**Result:** The **PCSCF Tables** window is displayed.

- 2 In the left pane, expand the **IBC Route Profile** folder.

**Result:** The IBC Route Profile Tables are listed under the folder in the left pane.

If the folder is empty, add a IBC Route Profile Table.

Perform the following steps in the **PCSCF Tables** window to add, rename, or delete a IBC Route Profile Table :

| If you want to ...             | then ...   |
|--------------------------------|--|
| add a IBC Route Profile Table, | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |

| If you want to ...                | then ...   |
|-----------------------------------|--|
| rename a IBC Route Profile Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a IBC Route Profile Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a IBC Route Profile Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.  
Add the IBC Route Profile Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.
- 4 Perform the following steps at the **PCSCF Tables** window to add, modify, or delete the IBC Route Profile Table attributes:

| If you want to ...                          | then ...  |
|---|---|
| add the IBC Route Profile Table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                           | then ...   |
|--|--|
| modify a IBC Route Profile Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a IBC Route Profile Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>            |

**5** Provision the following parameters:

| Parameter   | Provisioning  |
|---|---|
| <b>Profile Id</b>                                   | In the <b>Profile Id</b> field, select a Route Profile ID.  |
| <b>Description</b>                                  | In the <b>Description</b> field, enter a brief description up to 15 characters.   |
| <b>Pre-Routing Calling Digit Manipulation Table</b> | In the <b>Pre-Routing Calling Digit Manipulation Table</b> list, select the IMS Digit Table ID that you want to associate to this profile .<br>Pre-Routing Calling Digit Manipulation Table must point to a valid IMS Digit Table if nonzero. |
| <b>Pre-Routing Called Digit Manipulation Table</b>  | In the <b>Pre-Routing Called Digit Manipulation Table</b> list, select the IMS Digit Table ID that you want to associate to this profile.<br>Pre-Routing Called Digit Manipulation Table must point to a valid IMS Digit Table if nonzero.    |

| Parameter  | Provisioning   |
|--|--|
| <b>Post-Routing Calling Digit Manipulation Table</b> | <p>In the <b>Post-Routing Calling Digit Manipulation Table</b> field, select the IMS Digit Table ID that you want to associate to this profile.</p> <p>Post-Routing Calling Digit Manipulation Table must point to a valid IMS Digit Table if nonzero.</p>   |
| <b>Post-Routing Called Digit Manipulation Table</b>  | <p>In the <b>Post-Routing Called Digit Manipulation Table</b> field, select the IMS Digit Table ID that you want to associate to this profile.</p> <p>Post-Routing Called Digit Manipulation Table must point to a valid IMS Digit Table if nonzero.</p>   |
| <b>Domain Re-write</b>                               | <p>In the <b>Domain Re-write</b> field, select No, Conditional, or Always as appropriate.</p> <p><b>Note:</b></p> <p>Cross-Check Verification</p> <ul style="list-style-type: none"> <li>• When Domain Rewrite is set to Conditional or Always, New Domain Name must be filled in.</li> <li>• When Domain Rewrite is set to Conditional, Domain Match must point to a valid IBC Domain Table.</li> </ul> |
| <b>New Domian Name</b>                               | <p>In the <b>New Domian Name</b> field, enter the new domain name.</p> <p><b>Note:</b></p> <p>Cross-Check Verification</p> <ul style="list-style-type: none"> <li>• New Domain Name if not empty, must follow valid FQDN format.</li> </ul>  |

| Parameter                                  | Provisioning  |
|--|---|
| <b>Originating Trunk Group Rewrite</b>     | <p>In the <b>Originating Trunk Group Rewrite</b> field, select Conditional or Always as appropriate.</p> <p><b>Note:</b></p> <p>Cross-Check Verification</p> <ul style="list-style-type: none"> <li>When Originating Trunk Group is set to Conditional or Always, New Originating Trunk Group Label and New Originating Trunk Group Context must be filled in.</li> <li>When Originating Trunk Group Rewrite or Destination Trunk Group Rewrite is set to Conditional, then Trunk Group field must point to a valid Trunk Group Table.</li> </ul> |
| <b>New Originating Trunk Group Label</b>   | <p>In the <b>New Originating Trunk Group Label</b> field, enter the trunk group label in the format defined in RFC 4904 for trunk-group-label.</p> <p>This field specifies the text to put into the “tgrp” parameter. If the Originating Trunk Group Rewrite is set to a value other than ‘No’, then this field must be filled in.</p>  |
| <b>New Originating Trunk Group Context</b> | <p>In the <b>New Originating Trunk Group Context</b> field, enter the trunk group context in the format defined in RFC 4904 for the descriptor of trunk-context, where descriptor is defined in RFC 3966 as part of phone-context (domain or telephone number).</p> <p>This field specifies the text to put into the “trunk-context” parameter. If “Originating Trunk Group Rewrite” is set a value other than ‘No’, then this field must be filled in.</p>   |
| <b>Destination Trunk Group Rewrite</b>     | <p>In the <b>Destination Trunk Group Rewrite</b> field, select No, Conditional, or Always as appropriate.</p> <p><b>Note:</b></p> <p>Cross-Check Verification</p> <ul style="list-style-type: none"> <li>When Destination Trunk Group is set to Conditional or Always, Destination Originating Trunk Group Label and New Originating Trunk Group Context must be filled in.</li> </ul>  |

| Parameter                                  | Provisioning   |
|--|--|
| <b>New Destination Trunk Group Label</b>   | <p>In the <b>New Destination Trunk Group Label</b> field, enter the trunk group label in the format defined in RFC4904 for trunk-group-label.</p> <p>This field specifies the text to put into the “tgrp” parameter. If the “Destination Trunk Group Rewrite” field is set to a value other than ‘No’, then this field must be filled in.</p>              |
| <b>New Destination Trunk Group Context</b> | <p>In the <b>New Destination Trunk Group Context</b> field, enter the trunk group context in the format defined in RFC4904 for trunk-group-label.</p> <p>This field specifies the text to put into the “trunk-context” parameter. If the “Destination Trunk Group Rewrite” field is set to a value other than ‘No’, then this field must be filled in.</p> |
| <b>Default Proxy</b>                       | <p>From the <b>Default Proxy</b> list, select the Target Group List ID you want to associate to this profile.</p> <p>Default Proxy must point to a valid Target Group List if non-zero.</p>  |
| <b>Routing Priority</b>                    | <p>Under <b>Routing Priority</b>, select the item and move it to prioritize as follows:</p> <p>Click <b>Move Up</b> to move the item up and assign higher priority.</p> <p>Click <b>Move Down</b> to move the item down and assign lower priority.</p>   |
| <b>CRF Route Profile ID</b>                | <p>From the <b>CRF Route Profile ID</b> list, select the IDs of the CRF Route profiles.</p>  |
| <b>Domain Match</b>                        | <p>From the <b>Domain Match</b> list, select the NEW IBC Domain Table ID that you want to associate to this profile.</p> <p>Domain Match must point to a valid IBC Domain Table if non-zero.</p>   |
| <b>Trunk Group</b>                         | <p>From the <b>Trunk Group</b> list, select the NEW Trunk Group List Table ID that you want to associate to this profile.</p> <p>Trunk Group must point to a valid Trunk Group Table if non-zero.</p>  |

| Parameter | Provisioning |
|-----------|--------------|
|           |              |

For more information on the parameters, see the topic **IBC Route Profile** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click **OK**.

**Result:** The IBC Route Profile Table attributes are provisioned successfully.

END OF STEPS

---

# To provision Target Group Table

## Purpose

This procedure describes the steps to provision a Target Group Table.

## Before you begin

### Note:

- Only one Target Group Table can be provisioned.
- Maximum 1024 Target Group records can be provisioned.

## Steps to provision a Target Group Table

Perform the following steps at the Provisioning GUI:

- 1** Select **IMS** → **IMS Components** → **PCSCF Tables**.

**Result:** The **PCSCF Tables** window is displayed.

- 2** In the left pane, expand the **Target Group** folder.

**Result:** The Target Group tables are listed under the folder in the left pane.

If the folder is empty, add a Target Group Table.

Perform the following steps in the **PCSCF Tables** window to add, rename, or delete a Target Group Table :

| If you want to ...        | then ...   |
|---------------------------|--|
| add a Target Group Table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...           | then ...  |
|------------------------------|---|
| rename a Target Group Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a Target Group Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Target Group Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>     |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the Target Group Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **PCSCF Tables** window to add, modify, or delete the Target Group Table attributes:

| If you want to ...                     | then ...  |
|--|---|
| add the Target Group Table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                      | then ...   |
|---|--|
| modify a Target Group Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a Target Group Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                |

**5** Provision the following parameters:

| Parameter            | Provisioning   |
|----------------------|--|
| <b>Group ID</b>      | In the <b>Group ID</b> field, select a group ID.   |
| <b>Description</b>   | In the <b>Description</b> field, enter a brief description up to 15 characters.  |
| <b>Location</b>      | From the <b>Location</b> list, select Access or Core.  |
| <b>Service Label</b> | <p>In the <b>Service Label</b> field, enter the service label up to 64 characters.</p> <p><b>Note:</b> If the Location type is Access, Service Label must be assigned to a specific IMS Service.</p>                                   |
| <b>P-CSCF GUL</b>    | <p>In the <b>P-CSCF GUL</b> field, enter the P-CSCF GUL in the format pcsf-xxxx.</p> <p><b>Note:</b> If the Location Type is Access, this must match one of the PCSCF Port Name on the IMS Service specified by the Service Label.</p> |
| <b>Target Type</b>   | From the <b>Target Type</b> list, select a IPv4 address, a IPv6 address, or a Domain.  |

| Parameter                         | Provisioning  |
|-----------------------------------|---|
| <b>Primary Target Host Name</b>   | In the <b>Primary Target Host Name</b> field, enter the Target Address.   |
| <b>Alternate Target Host Name</b> | In the <b>Alternate Target Host Name</b> field, enter the Target Address. |
| <b>Port</b>                       | In the <b>Port</b> field, enter the Port Number.                          |

| Parameter               | Provisioning  |
|-------------------------|---|
| <b>Enable Heartbeat</b> | <p>Select the <b>Enable Heartbeat</b> check box to enable heartbeat</p> <p><b>Note:</b></p> <p>Cross Verification</p> <ul style="list-style-type: none"> <li>• Service Label must be filled in when Location is Access.</li> <li>• Port must be 0 when Target Type is Domain.</li> <li>• P-CSCF GUL must be filled in when Location is Access.</li> <li>• P-CSCF GUL must be in the format of pcsf-xxxx where x are lowercase alphanumeric characters.</li> <li>• Primary Target Host Name must be filled in.</li> <li>• Primary Target Host Name and Alternate Target Host Name (if not blank) must be valid IPv4 address when Target Type is IPv4.</li> <li>• Primary Target Host Name and Alternate Target Host Name (if not blank) must be valid IPv6 address when Target Type is IPv6.</li> <li>• Primary Target Host Name must be valid Domain when Target Type is Domain. Alternate Target Host Name must be blank when Target Type is Domain.</li> <li>• Primary and Alternate Target Host Name cannot be same in one Target Group record.</li> <li>• The Target must be unique across different Target Group records. This includes, Unique Primary Target Host Name + Port for IPv4 and IPv6 Target Type Unique Alternate Target Host Name + Port for IPv4 and IPv6 Target Type Unique Primary Target Host Name for Domain Target Type</li> <li>• Location, Target Type, Primary Target Host Name and Alternate Target Host Name cannot be modified once provisioned.</li> <li>• The Target Group record cannot be deleted if being used by Target Group List.</li> </ul> |

For more information on the parameters, see the topic **Target Group** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The Target Group Table attributes are provisioned successfully.

END OF STEPS

---

# To provision Target Group List

## Purpose

This procedure describes the steps to provision a Target Group List.

## Before you begin

### Note:

- Only one Target Group List Table can be provisioned.
- Maximum 1024 Target Group List records can be provisioned.

## Steps to provision a Target Group List Table

Perform the following steps at the Provisioning GUI:

- 1** Select **IMS** → **IMS Components** → **PCSCF Tables**.

**Result:** The **PCSCF Tables** window is displayed.

- 2** In the left pane, expand the **Target Group List** folder.

**Result:** The Target Group List tables are listed under the folder in the left pane.

If the folder is empty, add a Target Group List Table.

Perform the following steps in the **PCSCF Tables** window to add, rename, or delete a Target Group List Table :

| If you want to ...             | then ...   |
|--------------------------------|--|
| add a Target Group List Table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                | then ...   |
|-----------------------------------|--|
| rename a Target Group List Table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a Target Group List Table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Target Group List Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>   |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the Target Group List Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **PCSCF Tables** window to add, modify, or delete the Target Group List Table attributes:

| If you want to ...                          | then ...  |
|---|---|
| add the Target Group List Table attributes, | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                           | then ...   |
|--|--|
| modify a Target Group List Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a Target Group List Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>            |

**5** Provision the following parameters:

| Parameter             | Provisioning  |
|-----------------------|---|
| <b>Group List ID</b>  | In the <b>Group List ID</b> field, select a Target Group List ID.               |
| <b>Description</b>    | In the <b>Description</b> field, enter a brief description up to 15 characters. |
| <b>Location</b>       | In the <b>Location</b> field, select Access, or Core.                           |
| <b>Group Affinity</b> | In the <b>Group Affinity</b> field, select the group affinity.                  |

| Parameter                | Provisioning  |
|--------------------------|---|
| <b>Target Group List</b> | <p>Under the <b>Target Group List</b> group, you can provision up to 20 Target groups.</p> <p>The table displays the following:</p> <ul style="list-style-type: none"><li>• Target Group ID</li><li>• Transport type</li><li>• Order</li><li>• Priority</li><li>• Weight</li></ul> <p><b>Note:</b></p> <p>Cross-Check Verification</p> <ul style="list-style-type: none"><li>• Each Target Group List Entry must have a Target Group ID from the Target Group Table that is associated with a Location type (Access or Core) that matches the Location specified in the Target Group List.</li><li>• If the same Target Group ID is added in the Target Group List, then the Transport Type must be different.</li><li>• The Location Type of the Target Group List cannot be modified once provisioned.</li><li>• A Target Group List cannot be deleted if being used by IBC Route Profile or IBC Domain table or Trunk Group table.</li></ul> |

For more information on the parameters, see the topic **Target Group List** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

6 Click **OK**.

**Result:** The Target Group List Table attributes are provisioned successfully.

END OF STEPS

# To provision IBC Domain Table

## Purpose

This procedure describes the steps to provision the IBC Domain Table.

## Before you begin

### Note:

- Maximum 256 IBC Domain Tables can be provisioned.
- In each IBC Domain Table, maximum 100 IBC Domain Entries can be provisioned. But the total number of IBC Domain records that can be provisioned in all IBC Domain Tables is limited to 4096.

## Steps to provision a IBC Domain Table

Perform the following steps at the Provisioning GUI:

- 1** Select **IMS** → **IMS Components** → **PCSCF Tables**.

**Result:** The **PCSCF Tables** window is displayed.

- 2** In the left pane, expand the **IBC Domain Table** folder.

**Result:** The IBC Domain Table tables are listed under the folder in the left pane.

If the folder is empty, add a IBC Domain Table.

Perform the following steps in the **PCSCF Tables** window to add, rename, or delete a IBC Domain Table :

| If you want to ...      | then ...   |
|-------------------------|--|
| add a IBC Domain Table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...         | then ...  |
|----------------------------|---|
| rename a IBC Domain Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a IBC Domain Table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a IBC Domain Table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>       |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the IBC Domain Table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **PCSCF Tables** window to add, modify, or delete the IBC Domain Table attributes:

| If you want to ...                   | then ...  |
|--------------------------------------|---|
| add the IBC Domain Table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                    | then ...   |
|---------------------------------------|--|
| modify a IBC Domain Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a IBC Domain Table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                |

**5** Provision the following parameters:

| Parameter        | Provisioning  |
|------------------|---|
| <b>Domain ID</b> | In the <b>Domain ID</b> field, select a Domain Routing record ID.   |
| <b>Domain</b>    | In the <b>Domain</b> field, enter the domain string.<br><b>Note:</b> It is case insensitive.  |
| <b>Next Hop</b>  | <p>In the <b>Next Hop</b> field, select a valid Target Group List.</p> <p><b>Note:</b></p> <p>Cross-Check Verification</p> <ul style="list-style-type: none"> <li>The Domain Name must be of valid Domain format</li> <li>The Domain Name must be unique across the IBC Domain records in the same IBC Domain Table.</li> <li>Domain Name cannot be modified once provisioned.</li> </ul> |

For more information on the parameters, see the topic **IBC Domain Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The IBC Domain Table attributes are provisioned successfully.

END OF STEPS

---

# To provision Trunk Group

## Purpose

This procedure describes the steps to provision a Trunk Group table.

## Before you begin

### Note:

- Up to 256 Trunk Group tables can be added in the system
- Each table can contain up to 100 Trunk Group entries. The total number of Trunk Group records in the system is limited to 4096.

## Steps to provision a Trunk Group table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → PCSCF Tables**.

**Result:** The **PCSCF Tables** window is displayed.

- 2 In the left pane, expand the **Trunk Group** folder.

**Result:** The Trunk Group tables are listed under the folder in the left pane.

If the folder is empty, add a Trunk Group table.

Perform the following steps in the **PCSCF Tables** window to add, rename, or delete a Trunk Group table :

| If you want to ...       | then ...  |
|--------------------------|---|
| add a Trunk Group table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...          | then ...  |
|-----------------------------|---|
| rename a Trunk Group table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a Trunk Group table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Trunk Group table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>      |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the Trunk Group table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **PCSCF Tables** window to add, modify, or delete the Trunk Group table attributes:

| If you want to ...                    | then ...  |
|---------------------------------------|---|
| add the Trunk Group table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                     | then ...   |
|--|--|
| modify a Trunk Group table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a Trunk Group table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                |

**5** Provision the following parameters:

| Parameter                | Provisioning  |
|--------------------------|---|
| <b>Trunk Group ID</b>    | In the <b>Trunk Group ID</b> field, select a Trunk Group ID.  |
| <b>Trunk Group Type</b>  | In the <b>Trunk Group Type</b> field, select Originating or Destination. This field specifies whether to analyze originating (Contact header) or destination (Request- URI) Trunk Group information.  |
| <b>Trunk Group Label</b> | In the <b>Trunk Group Label</b> field, enter a Trunk Group Label that corresponds to the definition from RFC 4904 for trunk-group-label.  |
| <b>Trunk Context</b>     | In the <b>Trunk Context</b> field, enter a Trunk Context that corresponds to the definition from RFC 4904 for the descriptor of trunk-context, where descriptor is defined in RFC 3966 as part of phone-context (domain or telephone number). |

| Parameter       | Provisioning   |
|-----------------|--|
| <b>Next Hop</b> | <p>In the <b>Next Hop</b> field, select the Trunk Group List ID associated with this profile.</p> <p><b>Note:</b></p> <p>Cross-Check Verification</p> <ul style="list-style-type: none"><li>• Trunk Group Label must be filled in and follow the definition from RFC4904 for trunk-group-label..</li><li>• Trunk Context must be filled in and follow the definition from RFC4904 for trunk-context</li><li>• The combination of Trunk Group Type, Trunk Group Label , and Trunk Context must be unique across all Trunk Group records in one Trunk Group table.</li><li>• Next Hop must point to a valid Target Group List.</li></ul> |

For more information on the parameters, see the topic **Trunk Group** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

6 Click **OK**.

**Result:** The Trunk Group table attributes are provisioned successfully.

END OF STEPS

# To provision ACL List

## Purpose

This procedure describes the steps to provision an ACL List.

## Before you begin

### Note:

- Up to 1024 ACL List tables can be added in the system
- Maximum 100 Source Info records can be provisioned. The total number of Source Info records in the system is limited to 4096

## Steps to provision a ACL List table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → PCSCF Tables**.

**Result:** The **PCSCF Tables** window is displayed.

- 2 In the left pane, expand the **ACL List** folder.

**Result:** The ACL List tables are listed under the folder in the left pane.

If the folder is empty, add a ACL List table.

Perform the following steps in the **PCSCF Tables** window to add, rename, or delete a ACL List table :

| If you want to ...    | then ...  |
|-----------------------|---|
| add a ACL List table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...       | then ...  |
|--------------------------|---|
| rename a ACL List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a ACL List table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a ACL List table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>         |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the ACL List table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **PCSCF Tables** window to add, modify, or delete the ACL List table attributes:

| If you want to ...                 | then ...  |
|------------------------------------|---|
| add the ACL List table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                  | then ...   |
|-------------------------------------|--|
| modify a ACL List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>PCSCF Tables</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a ACL List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                |

**5** Provision the following parameters:

| Parameter               | Provisioning  |
|-------------------------|---|
| <b>Source Info ID</b>   | In the <b>Source Info ID</b> field, select the Source Info ID.  |
| <b>IP Version Type</b>  | In the <b>IP Version Type</b> field, select IPv4 or IPv6. The default value is IPv4.                          |
| <b>Start IP Address</b> | In the <b>Start IP Address</b> field, enter the start IP address.   |
| <b>End IP Address</b>   | In the <b>End IP Address</b> field, enter the end IP address.   |
| <b>Lower Port</b>       | In the <b>Lower Port</b> field, enter the lower port number. The range is 0 to 65535. The default value is 0. |

| Parameter  | Provisioning   |
|------------|--|
| Upper Port | <p>In the <b>Upper Port</b> field, enter the upper port number. The range is 0 to 65535. The default value is 0.</p> <p><b>Note:</b></p> <p>Cross-Check Verification</p> <ul style="list-style-type: none"> <li>Start IP and End IP must match the selected IP Version Type.</li> <li>End IP must be greater than or equal to Start IP.</li> <li>Upper Port must be greater than or equal to Lower Port.</li> <li>Source Info entry cannot be modified once provisioned.</li> </ul> <p>Transport Range across the Source Info entries in the same ACL List, the following three cases are not allowed,</p> <ul style="list-style-type: none"> <li>Case 1: Two Source Info Entries have same IP + Port Range</li> <li>Case 2: One Source Info Entry's IP range is subset of another Source Info Entry's IP range</li> <li>Case 3: Two Source Info Entries have same IP Range, and one entry's Port Range is subset of the other's Port Range.</li> </ul> <p>Actually case 2 already describes case 1 and case 3, because same IP is an extreme case of IP subset.</p> <ul style="list-style-type: none"> <li>One Source Info Entry's IP range is subset of another Source Info Entry's IP range</li> <li>Two Source Info Entries have same IP Range, and one entry's Port Range is subset of the other's Port Range.</li> </ul> |

For more information on the parameters, see the topic **ACL List** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 6 Click **OK**.

**Result:** The ACL List table attributes are provisioned successfully.

END OF STEPS

# To provision iAGCF line OOS and CPC display functionalities

## Overview

### Purpose

This section describes the provisioning procedures for iAGCF Line OOS and CPC Display functionalities.

### Contents

|  |       |
|--|-------|
| <a href="#">To provision an AGCF CPC String to CPC Digit Table</a> | 5-328 |
|--|-------|

# To provision an AGCF CPC String to CPC Digit Table

## Purpose

This procedure is used to provision an AGCF CPC String to CPC Digit Table.

## Before you begin

Points to remember:

- Maximum number of tables allowed is 1.
- Maximum number of records allowed is 20.
- The last record cannot be deleted if any AGCF Profiles have the **Include CPC Digit in Caller ID** field set.

## Steps to provision an AGCF CPC String to CPC Digit table

Perform the following steps at the Provisioning GUI:

**1** Select **IMS → IMS Components → AGCF Tables**.

**Result:** The **AGCF Tables** window is displayed.

In the left pane, expand the **AGCF CPC String to CPC Digit** folder.

**Result:** The AGCF CPC String to CPC Digit table is listed under the folder in the left pane.

If the folder is empty, add an AGCF CPC String to CPC Digit table.

**2** Perform the following steps in the **AGCF Tables** window to add, rename, or delete an AGCF CPC String to CPC Digit table:

| If you want to..                           | then...  |
|--|--|
| add an AGCF CPC String to CPC Digit table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add AGCF CPC String to CPC Digit table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> |

| If you want to..                              | then...  |
|---|--|
| rename an AGCF CPC String to CPC Digit table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/> <b>Result:</b> The <b>Rename AGCF CPC String to CPC Digit table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of Steps.</i></p> |
| delete an AGCF CPC String to CPC Digit table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of Steps.</i></p>   |

- 3 Perform the following steps at the **AGCF Tables** window to add, modify, or delete the AGCF CPC String to CPC Digit table attributes:

| If you want to ...                                       | then ...  |
|--|---|
| add the AGCF CPC String to CPC Digit table attributes,   | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/> <b>Result:</b> The <b>AGCF CPC String to CPC Digit</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify an AGCF CPC String to CPC Digit table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/> <b>Result:</b> The <b>AGCF CPC String to CPC Digit</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                                       | then ...  |
|--|---|
| delete an AGCF CPC String to CPC Digit table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

4 Configure the following parameters

| Parameter         | Description   |
|-------------------|---|
| <b>CPC String</b> | <p>Enter the appropriate value in the <b>CPC String</b> field.</p> <p>This field defines the Calling Party Category String.</p> <p><b>Note:</b> CPC String cannot be blank and is NOT case sensitive.</p> |
| <b>CPC Digit</b>  | <p>Select the appropriate option from the <b>CPC Digit</b> list.</p> <p>This field defines the Calling Party Category Digit.</p>  |

5 Click **OK**.

**Result:** The AGCF CPC String to CPC Digit table attributes are provisioned successfully.

For more information on the parameter description, see the topic “AGCF CPC String to CPC Digit table” in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# To provision Access Transfer Control Function (ATCF) support

## Overview

### Purpose

This section describes the provisioning procedures for Access Transfer Control Function (ATCF) support.

### Contents

|                              |       |
|------------------------------|-------|
| To provision an STN-SR Table | 5-332 |
|------------------------------|-------|

# To provision an STN-SR Table

## Purpose

This procedure is used to provision an STN-SR Table.

## Description

It is the responsibility of the MSC to provision and manage the STR-SR to IP/port relationship. This relationship must be coordinated with the STN-SR table since it is specified on the p-cscf component. The ATCF matches the STN-SR included in the Request\_URI of the handover INVITE from the MSC. The subscriber number (tel url) or username (sip uri) is compared with the entry in the STN-SR table. The normalized form (without leading + in case of E.164, spaces, and other separator characters) is used. While locking it must be ensured that the p-cscf components are ATCF enabled. If the p-cscf being locked is the p-cscf that the MSC is using to serve the STN-SR, then all the ATCF service for that STN-SR is lost, even if the UE registers through another unlocked p-cscf on the same IMS service.

## Before you begin

### Points to remember

- A maximum of 64 unique STN-SR Identifiers are allowed in the new table.

## Steps to provision the STN-SR table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS → IMS Component → PCSCF Tables**.

**Result:** The **PCSCF Tables** window is displayed.

In the left pane, expand the **STN-SR List** folder.

**Result:** The STN-SR tables are listed under the folder in the left pane.

If the folder is empty, add an STN-SR table.

- 
- 2 Perform the following steps in the **PCSCF Tables** window to add, rename, or delete a STN-SR table :

| If you want to..        | then...  |
|-------------------------|--|
| add an STN-SR table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/> <b>Result:</b> The <b>Add STN-SR table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |
| rename an STN-SR table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/> <b>Result:</b> The <b>Rename STN-SR table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p>  |
| delete an STN-SR table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p>   |

3 Double-click the newly created table. The table opens in the right pane.

Perform the following steps at the **P-CSCF Tables** window to add, modify, or delete the STN-SR table attributes:

| If you want to ...               | then ...  |
|----------------------------------|---|
| add the STN-SR table attributes, | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/> <b>Result:</b> The <b>STN-SR Identifier</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 4</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                  | then ...   |
|-------------------------------------|--|
| modify the STN-SR table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>STN-SR Identifier</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a> to provision the parameters.<br/><i>End of steps</i></li> </ol> |
| delete the STN-SR table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.<br/><i>End of steps.</i></li> </ol>                     |

**4** Provision the following parameters.

| Parameter                | Description  |
|--------------------------|--|
| <b>STN-SR ID</b>         | In the <b>STN-SR ID</b> list, select the appropriate STN-SR ID value. This field defines the Id of the STN-SR Identifier.<br>The range is 1 to 64.   |
| <b>STN-SR Identifier</b> | Enter the appropriate value in the <b>STN-SR Identifier</b> field.<br>STN-SR is subscription information provided to HSS for each subscriber if SRVCC service is allowed by hPLMN. STN-SR is a routing number indicating the SCC-AS or the ATCF if SRVCC enhanced with ATCF is used. |

**5** Click **OK**.

**Result:** The STN-SR table attributes are provisioned successfully.

*Manage services*

*To provision Access Transfer Control Function (ATCF)  
support*

To provision an STN-SR Table

For more information , see the *Alcatel-Lucent Control Platform 1800/1000/5400 Configuration Database Interface Specification and Object Descriptions Manual*,  
275-900-379

E N D   O F   S T E P S

DRAFT

DRAFT

# To provision SIP heartbeat after failure to reach a network element

## Overview

### Purpose

This section describes the provisioning procedures to provision SIP heartbeat after failure to reach a network element.

### Contents

|   |       |
|---|-------|
| To provision an SIP Heartbeat after failure Exemption Table | 5-337 |
|---|-------|

# To provision an SIP Heartbeat after failure Exemption Table

## Purpose

This procedure is used to provision an SIP Heartbeat after failure Exemption Table.

## Before you begin

### Points to remember

- A maximum of 256 unique records is allowed.
- Duplicate records with the same "destination + port + transport" are not allowed.  
When an entry is added, the field "Destination Address Type" is bonded together with "Destination".

## Steps to provision the SIP Heartbeat after failure Exemption table

Perform the following steps at the Provisioning GUI:

**1** Select **IMS → IMS General Tables**.

**Result:** The **IMS General Tables** window is displayed.

In the left pane, expand the **SIP Heartbeat after failure Exemption Table** folder.

**Result:** The SIP Heartbeat after failure Exemption tables are listed under the folder in the left pane.

If the folder is empty, add an SIP Heartbeat after failure Exemption table.

**2** Perform the following steps in the **IMS General Tables** window to add, rename, or delete a SIP Heartbeat after failure Exemption table :

| If you want to..                                    | then...  |
|---|--|
| add an SIP Heartbeat after failure Exemption table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add SIP Heartbeat after failure Exemption table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.<br/><i>End of steps.</i></li> </ol> |

| If you want to..                                       | then...  |
|--|--|
| rename an SIP Heartbeat after failure Exemption table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename SIP Heartbeat after failure Exemption table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps.</i></p> |
| delete an SIP Heartbeat after failure Exemption table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p>   |

- 3 Double-click the newly created table. The table opens in the right pane.

Perform the following steps at the **IMS General Tables** window to add, modify, or delete the SIP Heartbeat after failure Exemption table attributes:

| If you want to ...   | then ...  |
|--|---|
| add the SIP Heartbeat after failure Exemption table attributes,    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Heartbeat after failure Exemption Table Attributes</b> window is displayed.</li> <li>Continue with to <a href="#">Step 4</a>provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify the SIP Heartbeat after failure Exemption table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SIP Heartbeat after failure Exemption Table attributes</b> window is displayed.</li> <li>Continue with <a href="#">Step 4</a>to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...   | then ...  |
|--|---|
| delete the SIP Heartbeat after failure Exemption table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

4 Provision the following parameters.

| Parameter                       | Description  |
|---------------------------------|--|
| <b>Entry ID</b>                 | In the <b>Entry ID</b> list, select the ID of each table entry value. The range is 1 to 256. The default value is 1.   |
| <b>Destination Address Type</b> | Enter the link destination type in the <b>STN-SR Identifier</b> field. The default value is FQDN. This field is used to determine what type of checks should be applied for the Destination field. |
| <b>Destination</b>              | In the <b>Destination</b> field, specify the FQDN or IP address of the destination.  |
| <b>Port Number</b>              | In the <b>Port Number</b> field, specify the link destination port number. It is any valid IP port number. The value blank is used for all ports.  |
| <b>Transport</b>                | In the <b>Transport</b> field specify the type of transport used by the link. TLS is included to support any UEs that cannot use https as recommended in RFC3261. The default value is “UDP”.      |

5 Click **OK**.

**Result:** The SIP Heartbeat after failure Exemption table attributes are provisioned successfully.

For more information , see the *Alcatel-Lucent Control Platform 1800/1000/5400 Configuration Database Interface Specification and Object Descriptions Manual*,  
275-900-379

E N D   O F   S T E P S

# Support Multiple Access Network Subnets on FEPH

## Overview

### Purpose

This section provides the various procedures for Multiple Access Network Subnets support on FEPH.

### Contents

|  |       |
|--|-------|
| <a href="#">Support multiple access network subnets on FEPH</a>          | 5-342 |
| <a href="#">To grow a new external access subnet</a>                     | 5-343 |
| <a href="#">To convert one ordinary subnet to external access subnet</a> | 5-360 |
| <a href="#">To degrow one external access subnet</a>                     | 5-371 |

# Support multiple access network subnets on FEPH

## Overview

This topic briefly describes the feature, “Support multiple access network subnets on FEPH”.

## Description

Earlier FEPH only supported single subnet, and different IMS services used the same subnet. With the introduction of this feature, FEPH supports multiple subnets, and different IMS services can be in different subnets when they use FEPH services. There is only one FEPH published service IP address in the same subnet for each version.

This feature covers the following functionalities.

- Growth subnet - Add a new subnet on FEPH which was not previously being used in the system  
See “[To grow a new external access subnet](#)” (p. 5-343) for more information.
- Convert subnet - Move an existing subnet that previously did not use the FEPH to now use the FEPH  
See “[To convert one ordinary subnet to external access subnet](#)” (p. 5-360) for more information.
- De-growth subnet - Delete one subnet which is no longer used on FEPH.  
See “[To degrow one external access subnet](#)” (p. 5-371) for more information.

The tool `fehpSubnetCvt` supports these three functionalities.

# To grow a new external access subnet

## Purpose

This topic describes the procedure to grow a new external access subnet.

## Before you begin

Before using fephSubnetCvt to perform FEPH subnet conversion, the system environment must be ready with the following:

- The state for all pairs of cards is InserviceActive/InserviceStbyHot.
- This tool can only be run in Active MI with root login, so it must be ensured that the “startMI” is run before doing conversion.
- FEPH service has been grown to the system.

**Note:** Before going through the following procedure, it is recommended that the **fephSubnetCvt -b** is run to backup the system configuration. If some failures are encountered during the following procedure, the **fephSubnetCvt -u i** is run to restore the network configuration that is backed up.

## Procedure

Perform the following steps:

---

### 1 Add new IPv4 and/or IPv6 subnets for the system.

fephSubnetCvt only converts the existing subnet to external access subnet. So before conversion, the subnet that must be changed to the external access subnet, must be added into the system first.

For adding IPv4 subnet, please refer the topic, “To add a new external IPv4 subnet” in the *Alcatel-Lucent 5400 Linux Control Platform Configuration Management guide*, 270-702-014.

**Example:** The following is an example for adding IPv4 subnet:

```
<dibc2-s00c03h0:root>/root/jli053:  
# ip_adm -a add_subnet -b 10.84.22.224 -m 255.255.255.240 -n DHSPP4 -  
s 5 -o 14 -t pnf2,snf3  
Executing: ip_adm -a add_subnet -b 10.84.22.224 -m 255.255.255.240 -  
n DHSPP4 -s 5 -o 14 -t pnf2,snf3  
Running ip_adm  
RCCavcmInhibitAdm: Request succeeded  
(forward): running /opt/LSS/sbin/scdm_adm --action check_health  
sorting metadata between MIs....  
checking metadata between MIs....  
done..  
(forward): running rm -rf /var/opt/lib/scdt/backup
```

```
(forward): running /opt/LSS/sbin/scdm_adm --action backup_config
(forward): running /opt/LSS/sbin/net4conf_adm --action add_external_
    subnet --subnetnum 5 --subnetbase
10.84.22.224 --subnetmask 255.255.255.240 --subnetname DHSPP4
(forward): running /opt/LSS/sbin/net4conf_adm --action set_
    redundancy_mode --subnetnum 5 --mode eipm_acm
(forward): running /opt/LSS/sbin/net4conf_adm --action set_subnet_
    gateway --subnetnum 5 --offset 14
(forward): running /opt/LSS/sbin/net4conf_adm --action set_external_
    transport --subnetnum 5 --transportid
pnf2,snf3
(forward): running /opt/LSS/sbin/net4conf_adm --action set_
    connectivity_address --subnetnum 5 --offset 14 --
priority 1
(forward): running /opt/LSS/sbin/netconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
(forward): running /opt/LSS/sbin/netconf_adm --action install_host_
    all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action install_host_
    all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
forward): running /opt/LSS/sbin/syncConfigDB -f -l
Command completed successfully.

"ip_adm -a add_subnet..." is successful. After testing, run "ip_adm -a commit".
Or you can backout via "ip_adm -a backout"
<dibc2-s00c03h0:root>/root/jli053:
# ip_adm -a commit
Executing: ip_adm -a commit
Running ip_adm
RCCavcmInhibitAdm: Request succeeded
(commit): running /opt/LSS/sbin/create_ht
Tue Mar 13 09:54:58 CST 2012 create_ht
```

Tue Mar 13 09:54:58 CST 2012 Saving backup files under /var/opt/lib/mtce/data

Tue Mar 13 09:54:58 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_host.data

Tue Mar 13 09:54:58 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_host.layout

Tue Mar 13 09:54:58 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_tim.data

Tue Mar 13 09:54:58 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_tim.layout

Tue Mar 13 09:54:58 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_srv.data

Tue Mar 13 09:54:58 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_srv.layout

Tue Mar 13 09:54:58 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_system.data

Tue Mar 13 09:54:58 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_system.layout

Tue Mar 13 09:54:58 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_def\_lib.ksh

(commit): running /opt/LSS/sbin/scdm\_adm --action sync\_config

(commit): running /opt/LSS/sbin/remote\_shell root 169.254.64.64 /opt/LSS/1 sbin/netconf\_adm --action generate\_host\_all

dibc2-s00c04h0: generating network configuration... done

dibc2-s00c01h4: generating network configuration... done

dibc2-s00c02h4: generating network configuration... done

dibc2-s00c03h0: generating network configuration... done

(commit): running /opt/LSS/sbin/remote\_shell root 169.254.64.64 /opt/LSS/sbin/svcconf\_adm --action generate\_host\_all

dibc2-s00c04h0: generating service configuration... done

dibc2-s00c01h4: generating service configuration... done

dibc2-s00c02h4: generating service configuration... done

dibc2-s00c03h0: generating service configuration... done

(commit): running /opt/LSS/sbin/remote\_shell root 169.254.64.64 'export PATH=/opt/LSS/sbin:/opt/LSS/bin:/opt/LU3P/sbin:/opt/LU3P/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/java/bin:/opt/LSS/sbin:/opt/LSS/bin ; /opt/LSS/sbin/create\_ht'

Tue Mar 13 09:55:05 CST 2012 create\_ht

Tue Mar 13 09:55:05 CST 2012 Saving backup files under /var/opt/lib/mtce/data

Tue Mar 13 09:55:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_host.data

Tue Mar 13 09:55:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_host.layout

Tue Mar 13 09:55:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_tim.data

Tue Mar 13 09:55:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce\_tim.layout

---

```

Tue Mar 13 09:55:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.data
Tue Mar 13 09:55:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.layout
Tue Mar 13 09:55:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.data
Tue Mar 13 09:55:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.layout
Tue Mar 13 09:55:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    def_lib.ksh
(commit): running /opt/LSS/sbin/scdm_adm --action commit_config
(commit): running clr_rcc_inhibit
"ip_adm -a commit" completed successfully.

```

The following is an example for adding IPv6 subnet:

For adding IPv6 subnet, please refer the topic, “To add a new external IPv6 subnet” in the *Alcatel-Lucent 5400 Linux Control Platform Configuration Management guide*, 270-702-014.

Set the transport id to “pnf2,snf3”.

```

<dibc2-s00c03h0:root>/root/jli053:
# ip_adm -a add_subnet -b 2620:0:60:401F:0:0:0:490 -m 124 -n
    DHSPP46 -s 11 -o 2620:0:60:401F:0:0:0:4AE -t
pnf2,snf3
Executing: ip_adm -a add_subnet -b 2620:0:60:401F:0:0:0:490 -m 124 -
    n DHSPP46 -s 11 -o
2620:0:60:401F:0:0:0:49E -t pnf2,snf3
Running ip_adm
RCCavcmInhibitAdm: Request succeeded
(forward): running /opt/LSS/sbin/scdm_adm --action check_health
sorting metadata between MIs....
checking metadata between MIs....
done..
(forward): running rm -rf /var/opt/lib/scdt/backup
(forward): running /opt/LSS/sbin/scdm_adm --action backup_config
(forward): running /opt/LSS/sbin/net6conf_adm --action add_external_
    subnet --subnetnum 11 --subnetprefix
2620:0:60:401F:0:0:0:490 --prefixlength 124 --subnetname DHSPP46
(forward): running /opt/LSS/sbin/net6conf_adm --action set_
    redundancy_mode --subnetnum 11 --mode eipm_acm
(forward): running /opt/LSS/sbin/net6conf_adm --action set_subnet_
    gateway --subnetnum 11 --address6
2620:0:60:401F:0:0:0:49E
(forward): running /opt/LSS/sbin/net6conf_adm --action set_external_
    transport --subnetnum 11 --transportid
pnf2,snf3
(forward): running /opt/LSS/sbin/net6conf_adm --action set_
    connectivity_address --subnetnum 11 --address6
2620:0:60:401F:0:0:0:49E --priority 1
(forward): running /opt/LSS/sbin/netconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating network configuration... done

```

```

dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
(forward): running /opt/LSS/sbin/netconf_adm --action install_host_
    all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action install_host_
    all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
(forward): running /opt/LSS/sbin/syncConfigDB -f -l
Command completed successfully.

"ip_adm -a add_subnet..." is successful. After testing, run "ip_adm -
    a commit".
Or you can backout via "ip_adm -a backout"
<dibc2-s00c03h0:root>/root/jli053:
# ip_adm -a commit
Executing: ip_adm -a commit
Running ip_adm
RCCavcmInhibitAdm: Request succeeded
(commit): running /opt/LSS/sbin/create_ht
Tue Mar 13 10:17:37 CST 2012 create_ht
Tue Mar 13 10:17:37 CST 2012 Saving backup files under /var/opt/lib/
    mtce/data
Tue Mar 13 10:17:37 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.data
Tue Mar 13 10:17:37 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.layout
Tue Mar 13 10:17:37 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.data
Tue Mar 13 10:17:37 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.layout
Tue Mar 13 10:17:37 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.data
Tue Mar 13 10:17:37 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.layout
Tue Mar 13 10:17:37 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.data
Tue Mar 13 10:17:37 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.layout

```

```
Tue Mar 13 10:17:37 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    def_lib.ksh
(commit): running /opt/LSS/sbin/scdm_adm --action sync_config
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/netconf_adm --action
generate_host_all
dibc2-s00c04h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c03h0: generating network configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/svcconf_adm --action
generate_host_all
dibc2-s00c04h0: generating service 1 configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c03h0: generating service configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64
    'export
PATH=/opt/LSS/sbin:/opt/LSS/bin:/opt/LU3P/sbin:/opt/LU3P/bin:/usr/
    sbin:/usr/bin:/sbin:/bin:/usr/java/bin:/opt/LSS/sbin:/opt/LSS/
    bin ; /opt/LSS/sbin/create_ht'
Tue Mar 13 10:17:44 CST 2012 create_ht
Tue Mar 13 10:17:44 CST 2012 Saving backup files under /var/opt/lib/
    mtce/data
Tue Mar 13 10:17:44 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.data
Tue Mar 13 10:17:44 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.layout
Tue Mar 13 10:17:44 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.data
Tue Mar 13 10:17:44 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.layout
Tue Mar 13 10:17:44 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.data
Tue Mar 13 10:17:44 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.layout
Tue Mar 13 10:17:44 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.data
Tue Mar 13 10:17:44 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.layout
Tue Mar 13 10:17:44 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    def_lib.ksh
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/net6conf_adm --action
generate_host_all
dibc2-s00c04h0: generating network configuration... done
dibc2-s00c03h0: generating network configuration... done
(commit): running /opt/LSS/sbin/scdm_adm --action commit_config
(commit): running clr_rcc_inhibit
"ip_adm -a commit" completed successfully.
```

## 2 Add new IPv4 and/or IPv6 published IP for FEPH.

Use fehpSubnetCvt -a to add new IPv4 and/or IPv6 published IP on the new subnet for FEPH.

**Example:** The following is an example for adding new published IP on the new subnet for FEPH:

```
<dibc2-s00c03h0:root>/root/jli053:  
# fehpSubnetCvt -a  
fehpSubnetCvt: started 03/13/12 10:29  
Align RCC VMs  
RCCavcmInhibitAdm: Requested mode already set  
RCCavcmInhibitAdm: Requested mode already set  
Enabled MI switchover  
All RCC VM's are now aligned  
Add IPv4 or IPv6 subnet to the FEPH Service (Enter 4, 6, or q to  
quit): 4  
Available IPv4 subnets:  
IPv4 subnet number 1, subnet base 135.252.135.160, subnet mask  
255.255.255.240, subnet name OAM4  
IPv4 subnet number 2, subnet base 10.84.22.192, subnet mask  
255.255.255.240, subnet name Sig4Access  
IPv4 subnet number 3, subnet base 10.84.22.208, subnet mask  
255.255.255.240, subnet name Sig4Core  
IPv4 subnet number 4, subnet base 169.254.126.0, subnet mask  
255.255.255.0, subnet name vlan325 subnet  
IPv4 subnet number 5, subnet base 10.84.22.224, subnet mask  
255.255.255.240, subnet name DHSPP4  
IPv4 subnets currently assigned to FEPH:  
service type fehp, pool number 0, floater number 0, IPv4 subnet  
number 2, NI type published, offset 5, IPv4 IP address  
10.84.22.197  
IPv4 subnet number to be added FEPH Service: 5  
Enter IPv4 offset for FEPH Service: 1  
Executing: ip_adm -a add_floating_ip 1 -t fehp -i 0 -s 5 -o 1 -n  
published  
(checkmonitor): fehp has a monitor type of rem  
Running ip_adm  
RCCavcmInhibitAdm: Request succeeded  
(forward): running /opt/LSS/sbin/scdm_adm --action check_health  
sorting metadata between MIs....  
checking metadata between MIs....  
done..  
(forward): running rm -rf /var/opt/lib/scdt/backup  
(forward): running /opt/LSS/sbin/scdm_adm --action backup_config  
(forward): running /opt/LSS/sbin/net4conf_adm --action add_service_  
address --servicetype fehp --poolnum 0 --nitype unassigned --  
floaternum 0 --subnetnum 5 --offset 1  
(forward): running /opt/LSS/sbin/netconf_adm --action generate_host_  
all
```

```

dibc2-s00c03h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
(forward): running /opt/LSS/sbin/netconf_adm --action install_host_
    all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action install_host_
    all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
(forward): running rt4conf_adm --action add_service_address --
    servicetype feph --poolnum 0 --subnetnum 5 --floaternum 0 --
    offset 1 --nitype unassigned
(forward): running RTCONF_COMPLETE=1
(forward): running /opt/LSS/sbin/syncConfigDB -f -1
Command completed successfully.
(forward): running /opt/LSS/sbin/net4conf_adm --action add_service_
    address --servicetype feph --poolnum 0 --nitype published --
    floaternum 0 --subnetnum 5 --offset 1 --reuse
(forward): running /opt/LSS/sbin/net4conf_adm --action del_service_
    address --servicetype feph --poolnum 0 --nitype unassigned --
    floaternum 0 --subnetnum 5 --offset 1
(forward): running /opt/LSS/sbin/dnsconf_adm --action add_service_
    address4 --servicetype feph --poolnum 0 --floaternum 0 --
    subnetnum 5 --nitype published --offset 1
(forward): running DNS_COMPLETE=1
(forward): running /opt/LSS/sbin/netconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done

```

```

(forward) : running /opt/LSS/sbin/netconf_adm 1 --action install_host_
    all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward) : running /opt/LSS/sbin/svcconf_adm --action install_host_
    all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
(forward) : running rt4conf_adm --action add_service_address --
    servicetype feph --poolnum 0 --subnetnum 5 --floaternum 0 --
    offset 1 --nitype published
(forward) : running RTCONF_COMPLETE=1
(forward) : running /opt/LSS/sbin/syncConfigDB -f -l
Command completed successfully.
(ssh_conf_adm) : Running "/opt/LSS/sbin/sshconf_adm --action key_host_
    all"
dibc2-s00c03h0: generating SSH keys... done
dibc2-s00c01h4: generating SSH keys... done
dibc2-s00c02h4: generating SSH keys... done
dibc2-s00c04h0: generating SSH keys... done
dibc2-s00c15h0: aquiring SSH keys... done
(ssh_conf_adm) : Running "/opt/LSS/sbin/sshconf_adm --action generate_
    member_instance --servicetype feph --poolnum 0"
dibc2-s00c01h4: generating SSH daemon configuration... done
dibc2-s00c02h4: generating SSH daemon configuration... done
(ssh_conf_adm) : Running "/opt/LSS/sbin/sshconf_adm --action install_
    member_instance --servicetype feph --poolnum 0"
dibc2-s00c01h4: installing SSH daemon configuration... done
dibc2-s00c02h4: installing SSH daemon configuration... done
(ssh_conf_adm) : Running "/opt/LSS/sbin/sshconf_adm --action control_
    member_instance --servicetype feph --poolnum 0 --command restart"
dibc2-s00c01h4: restart non root internal fixed ... done
dibc2-s00c01h4: restart root only internal fixed ... done
dibc2-s00c02h4: restart non root internal fixed ... done
dibc2-s00c02h4: restart root only internal fixed ... done
(ssh_conf_adm) : Running sshconf_adm on OTHER_MI
dibc2-s00c01h4: generating SSH daemon configuration... done
dibc2-s00c02h4: generating SSH daemon configuration... done
"ip_adm -a add_floating_ip..." is successful. After testing, run "ip_
    adm -a commit".
Or you can backout via "ip_adm -a backout"
Executing: ip_adm -a commit
(checkmonitor) : feph has a monitor type of rem
Running ip_adm
RCCavcmInhibitAdm: Request succeeded
(commit) : running /opt/LSS/sbin/create_ht

```

```

Tue Mar 13 10:35:16 CST 2012 create_ht
Tue Mar 13 10:35:16 CST 2012 Saving backup files under /var/opt/lib/
    mtce/data
Tue Mar 13 10:35:16 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.data
Tue Mar 13 10:35:16 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.layout
Tue Mar 13 10:35:16 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.data
Tue Mar 13 10:35:16 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.layout
Tue Mar 13 10:35:16 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.data
Tue Mar 13 10:35:16 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.layout
Tue Mar 13 10:35:16 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.data
Tue Mar 13 10:35:16 CST 2012 Wrote new /var/opt/lib/
    mtce/data/1 mtce_system.layout
Tue Mar 13 10:35:16 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    def_lib.ksh
(commit): running /opt/LSS/sbin/scdm_adm --action sync_config
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/netconf_adm --action
generate_host_all
dibc2-s00c04h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c03h0: generating network configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/svcconf_adm --action
generate_host_all
dibc2-s00c04h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c03h0: generating service configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64
    'export
PATH=/opt/LSS/sbin:/opt/LSS/bin:/opt/LU3P/sbin:/opt/LU3P/bin:/usr/
    sbin:/usr/bin:/sbin:/bin:/usr/java/bin:/opt/LSS/sbin:/opt/LSS/
    bin ; /opt/LSS/sbin/create_ht'
Tue Mar 13 10:35:23 CST 2012 create_ht
Tue Mar 13 10:35:23 CST 2012 Saving backup files under /var/opt/lib/
    mtce/data
Tue Mar 13 10:35:23 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.data
Tue Mar 13 10:35:23 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.layout
Tue Mar 13 10:35:23 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.data
Tue Mar 13 10:35:23 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.layout

```

```

Tue Mar 13 10:35:23 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.data
Tue Mar 13 10:35:23 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.layout
Tue Mar 13 10:35:23 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.data
Tue Mar 13 10:35:23 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.layout
Tue Mar 13 10:35:23 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    def_lib.ksh
(commit): running /opt/LSS/sbin/scdm_adm --action commit_config
(commit): running clr_rcc_inhibit
"ip_adm -a commit" completed successfully.
Successful to add a new IPv4 floating ip to FEPH, subnet id = 5,
    service ip offset = 1
IPv4 subnets currently assigned to FEPH:
service type feph, pool number 0, floater number 0, IPv4 subnet
    number 2, NI type published, offset 5, IPv4 IP
address 10.84.22.197
service type feph, pool number 0, floater number 0, IPv4 subnet
    number 5, NI type published, offset 1, IPv4 IP address 10.84.22.225
Add IPv4 or IPv6 subnet to the FEPH Service (Enter 4, 6, or q to
    quit): 6
Available IPv6 subnets:
IPv6 subnet number 10, subnet prefix 2620:0:60:401F:0:0:0:470,
    prefix length 124, subnet name Bear6Core
IPv6 subnet number 11, subnet prefix 2620:0:60:401F:0:0:0:490,
    prefix length 124, subnet name DHSPP46
IPv6 subnet number 7, subnet prefix 2620:0:60:401F:0:0:0:410, prefix
    length 124, subnet name Sig6Access
IPv6 subnet number 8, subnet prefix 2620:0:60:401F:0:0:0:430, prefix
    length 124, subnet name Sig6Core
IPv6 subnet number 9, subnet prefix 2620:0:60:401F:0:0:0:450, prefix
    length 124, subnet name Bear6Access
IPv6 subnets currently assigned to FEPH:
service type feph, pool number 0, floater number 0, IPv6 subnet
    number 7, IPv6 IP address
2620:0:60:401F:0:0:0:417, NI type published
IPv6 subnet number to be added FEPH Service: 11
Enter IPv6 service ip for FEPH Service: 2620:0:60:401F:0:0:0:491
Executing: ip_adm -a add_floating_ip -t feph -i 0 -s 11 -o 2620:0:60:
    401F:0:0:0:491 -n published
(checkmonitor): feph 1 has a monitor type of rem
Running ip_adm
RCCavcmInhibitAdm: Request succeeded
(forward): running /opt/LSS/sbin/scdm_adm --action check_health
sorting metadata between MIs....
checking metadata between MIs....
done..
(forward): running rm -rf /var/opt/lib/scdt/backup
(forward): running /opt/LSS/sbin/scdm_adm --action backup_config

```

```
(forward): running /opt/LSS/sbin/net6conf_adm --action add_service_
    address --servicetype feph --poolnum 0 --nitype unassigned --
    floatternum 0 --subnetnum 11 --address6 2620:0000:0060:401f:0000:
    0000:0000:0491
(forward): running /opt/LSS/sbin/netconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
(forward): running /opt/LSS/sbin/net6conf_adm --action generate_host_
    all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/net6conf_adm --action install_host_
    all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/netconf_adm --action install_host_
    all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action install_host_
    all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
(forward): running rt6conf_adm --action add_service_address --
    servicetype feph --poolnum 0 --subnetnum 11 --floatternum 0 --
    address6 2620:0000:0060:401f:0000:0000:0491 --nitype
    unassigned
(forward): running RTCONF_COMPLETE=1
(forward): running /opt/LSS/sbin/syncConfigDB -f -l
Command completed successfully.
(forward): running /opt/LSS/sbin/net6conf_adm --action add_service_
    address --servicetype feph --poolnum 0 --nitype published --
    floatternum 0 --subnetnum 11 --address6 2620:0000:0060:401f:0000:
    0000:0000:0491 --reuse
(forward): running /opt/LSS/sbin/net6conf_adm --action del_service_
    address --servicetype feph --poolnum 0 --nitype unassigned --
    floatternum 0 --subnetnum 11 --address6 2620:0000:0060:401f:0000:
    0000:0000:0491
```

```

(forward): running /opt/LSS/sbin/dnsconf_adm --action add_service_
address6 --servicetype feph --poolnum 0 --floaternum 0 --
subnetnum 11 --nitype published --address6 2620:0000:0060:401f:-
0000:0000:0000:0491
(forward): running DNS_COMPLETE=1
(forward): running /opt/LSS/sbin/netconf_adm --action generate_host_
all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm 1 --action generate_
host_all
dibc2-s00c03h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
(forward): running /opt/LSS/sbin/net6conf_adm --action generate_host_
all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/net6conf_adm --action install_host_
all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/netconf_adm --action install_host_
all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action install_host_
all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
(forward): running rt6conf_adm --action add_service_address --
servicetype feph --poolnum 0 --subnetnum 11 --
floaternum 0 --address6 2620:0000:0060:401f:0000:0000:0000:0491 --
nitype published
(forward): running RTCONF_COMPLETE=1
(forward): running /opt/LSS/sbin/syncConfigDB -f -l
Command completed successfully.
(ssh_conf_adm): Running "/opt/LSS/sbin/sshconf_adm --action key_host_
all"
dibc2-s00c03h0: generating SSH keys... done
dibc2-s00c01h4: generating SSH keys... done
dibc2-s00c02h4: generating SSH keys... done
dibc2-s00c04h0: generating SSH keys... done
dibc2-s00c15h0: aquiring SSH keys... done

```

```
(ssh_conf_adm): Running "/opt/LSS/sbin/sshconf_adm --action generate_
    member_instance --servicetype feph --poolnum 0"
dibc2-s00c01h4: generating SSH daemon configuration... done
dibc2-s00c02h4: generating SSH daemon configuration... done
(ssh_conf_adm): Running "/opt/LSS/sbin/sshconf_adm --action install_
    member_instance --servicetype feph --poolnum 0"
dibc2-s00c01h4: installing SSH daemon configuration... done
dibc2-s00c02h4: installing SSH daemon configuration... done
(ssh_conf_adm): Running "/opt/LSS/sbin/sshconf_adm --action control_
    member_instance --servicetype feph --poolnum 0 --command restart"
dibc2-s00c01h4: restart non root internal fixed ... done
dibc2-s00c01h4: restart root only internal fixed ... done
dibc2-s00c02h4: restart non root internal fixed ... done
dibc2-s00c02h4: restart root only internal fixed ... done
(ssh_conf_adm): Running sshconf_adm on OTHER_MI
dibc2-s00c01h4: generating SSH daemon configuration... done
dibc2-s00c02h4: generating SSH daemon configuration... done
"ip_adm -a add_floating_ip..." is successful. After testing, run "ip_
    adm -a commit".
Or you can backout via "ip_adm -a backout"
Executing: ip_adm -a commit
(checkmonitor): feph has a monitor type of rem
Running ip_adm
RCCavcmInhibitAdm: R 1 equest succeeded
(commit): running /opt/LSS/sbin/create_ht
Tue Mar 13 10:48:05 CST 2012 create_ht
Tue Mar 13 10:48:05 CST 2012 Saving backup files under /var/opt/lib/
    mtce/data
Tue Mar 13 10:48:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.data
Tue Mar 13 10:48:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.layout
Tue Mar 13 10:48:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.data
Tue Mar 13 10:48:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.layout
Tue Mar 13 10:48:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.data
Tue Mar 13 10:48:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.layout
Tue Mar 13 10:48:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.data
Tue Mar 13 10:48:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.layout
Tue Mar 13 10:48:05 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    def_lib.ksh
(commit): running /opt/LSS/sbin/scdm_adm --action sync_config
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/netconf_adm --action
generate_host_all
dibc2-s00c04h0: generating network configuration... done
```

```

dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c03h0: generating network configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/svcconf_adm --action
generate_host_all
dibc2-s00c04h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c03h0: generating service configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64
    'export
PATH=/opt/LSS/sbin:/opt/LSS/bin:/opt/LU3P/sbin:/opt/LU3P/bin:/usr/
    sbin:/usr/bin:/sbin:/bin:/usr/java/bin:/opt/LSS/sbin:/opt/LSS/
    bin ; /opt/LSS/sbin/create_ht'
Tue Mar 13 10:48:12 CST 2012 create_ht
Tue Mar 13 10:48:12 CST 2012 Saving backup files under /var/opt/lib/
    mtce/data
Tue Mar 13 10:48:12 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.data
Tue Mar 13 10:48:12 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.layout
Tue Mar 13 10:48:12 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.data
Tue Mar 13 10:48:12 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.layout
Tue Mar 13 10:48:12 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.data
Tue Mar 13 10:48:12 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.layout
Tue Mar 13 10:48:12 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.data
Tue Mar 13 10:48:12 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.layout
Tue Mar 13 10:48:12 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    def_lib.ksh
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/net6conf_adm --action
generate_host_all
dibc2-s00c04h0: generating network configuration... done
dibc2-s00c03h0: generating network configuration... done
(commit): running /opt/LSS/sbin/scdm_adm --action commit_config
(commit): running clr_rcc_inhibit
"ip_adm -a commit" completed successfully.
Successful to add a new IPv6 floating ip to FEPH, subnet id = 11,
    service ip = 2620:0:60:401F:0:0:0:491
IPv6 subnets currently assigned to FEPH:
service type feph, pool number 0, floater number 0, IPv6 subnet
    number 11, IPv6 IP address
2620:0000:0060:401f:0000:0000:0491, NI type published
service type feph, pool number 0, floater number 0, IPv6 subnet
    number 7, IPv6 IP address

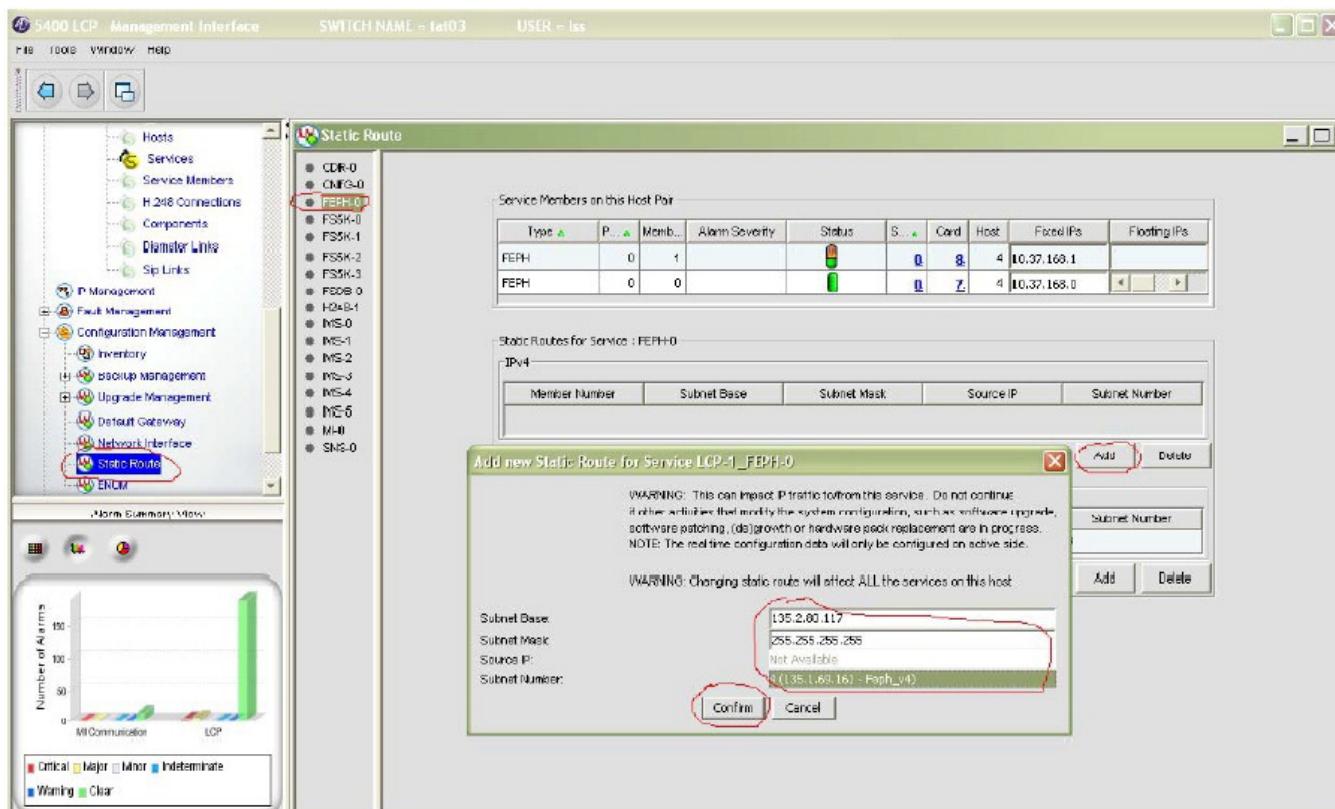
```

```
2620:0:60:401F:0:0:0:417, NI type published
Add IPv4 or IPv6 subnet to the FEPH Service 1 (Enter 4, 6, or q to
quit): q
fephSubnetCvt.ksh: Completed Successfully.
fephSubnetCvt.ksh Log: /var/opt/log/fephSubnetCvt/fephSubnetCvt.log
fephSubnetCvt.ksh ended 03/13/12 10:50.
```

### 3 Add IPv4 and/or IPv6 static route for the new subnet on FEPH.

After adding published IP for the new subnet on FEPH, some static routes must be added for the new subnets on FEPH by the MIGUI.

The following figure shows the process of adding IPv4 static route for the new subnet on FEPH.

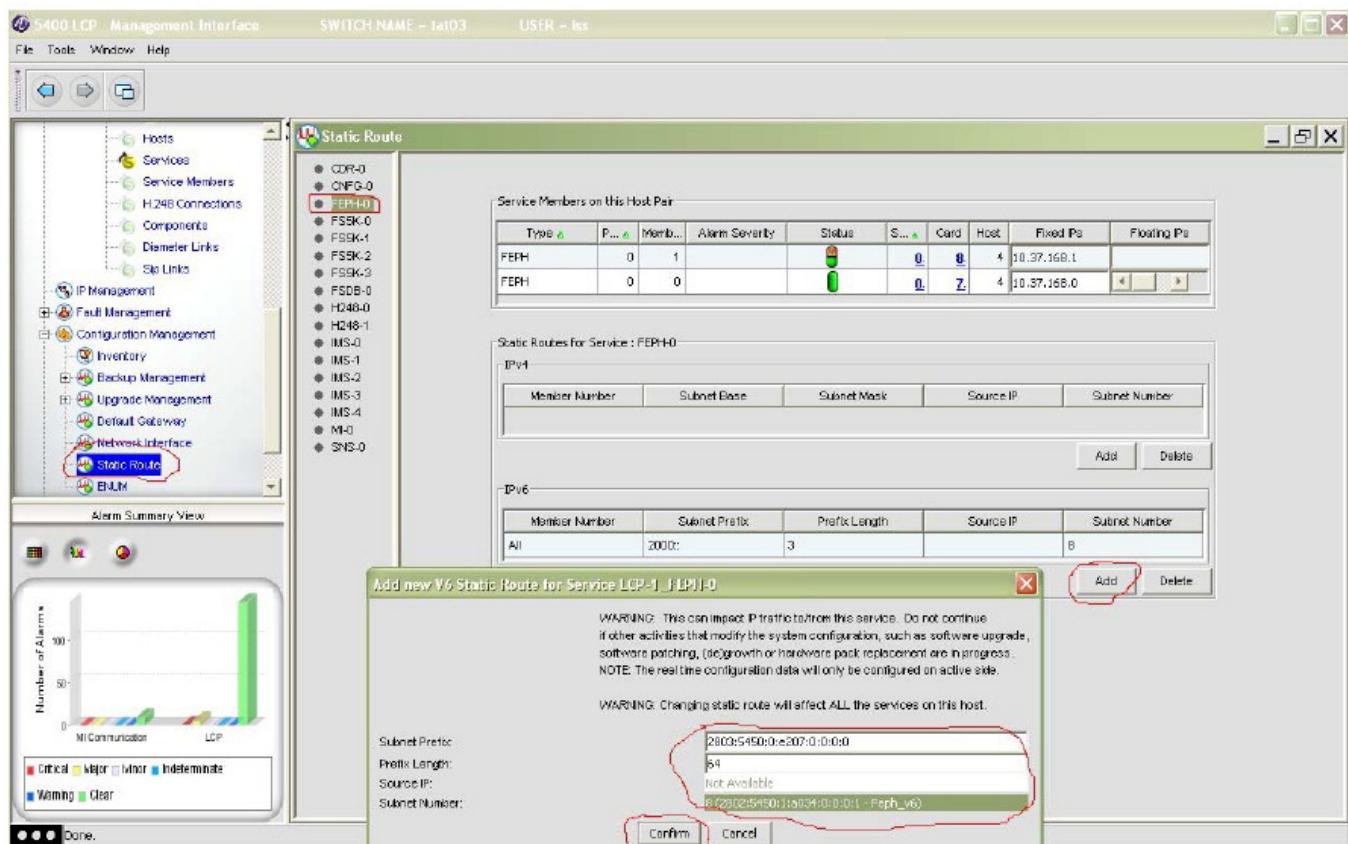


## Manage services

Support Multiple Access Network Subnets on FEPH

To grow a new external access subnet

The following figure shows the process of adding IPv6 static route for the new subnet on FEPH.



## 4 Enable FEPH service on the new external access subnet for IMS service.

For the detail procedure, see “[To grow Signaling Firewall and FEPH on a new network](#)” (p. 5-191).

E N D O F S T E P S

# To convert one ordinary subnet to external access subnet

## Purpose

This topic describes the procedure to convert one ordinary subnet to external access subnet.

## Before you begin

Before using fephSubnetCvt to perform FEPH subnet conversion, the system environment must be ready with the following:

- The state for all pairs of cards is InserviceActive/InserviceStbyHot.
- This tool can only be run in Active MI with root login, so it must be ensured that the “startMI” is run before doing conversion.
- FEPH service has been grown to the system.

**Note:** Before going through the following procedure, it is recommended that the **fephSubnetCvt -b** is run to backup the system configuration. If some failures are encountered during the following procedure, the **fephSubnetCvt -u i** is run to restore the network configuration that is backed up.

## Procedure

Perform the following steps:

---

### 1 Add new IPv4 and/or IPv6 published IP for FEPH.

Run fephSubnetCvt -c to convert a subnet, which is being used by IMS service, to external access subnet.

**Example:** The following is an example to convert a subnet to external access subnet:

```
<dibc2-s00c03h0:root>/root/jli053:  
# fephSubnetCvt -c  
fephSubnetCvt.ksh: started 03/13/12 16:16  
Align RCC VMs  
RCCavcmInhibitAdm: Requested mode already set  
RCCavcmInhibitAdm: Requested mode already set  
Enabled MI switchover  
All RCC VM's are now aligned  
IMS services currently not using FEPH:  
ims pool number 3, subnet number 5, IP version IPv4, ims service ip  
10.84.22.226  
ims pool number 3, subnet number 11, IP version IPv6, ims 1 service  
ip 2620:0000:0060:401f:0000:0000:0492  
Please enter the ims pool number which you want to convert the  
subnet to external access subnet: 3  
Please enter the IPv4 offset for feph service in subnet number 5:1
```

```

Please enter the IPv6 service IP for FEPH in subnet number 11:2620:
0000:0060:401f:0000:0000:0000:0491
Executing: ip_adm -a add_floating_ip -t feph -i 0 -s 5 -o 1 -n
published
(chckmonitor): feph has a monitor type of rem
Running ip_adm
RCCavcmInhibitAdm: Request succeeded
(forward): running /opt/LSS/sbin/scdm_adm --action check_health
sorting metadata between MIs....
checking metadata between MIs....
done..
(forward): running rm -rf /var/opt/lib/scdt/backup
(forward): running /opt/LSS/sbin/scdm_adm --action backup_config
(forward): running /opt/LSS/sbin/net4conf_adm --action add_service_
address --servicetype feph --poolnum 0 --nitype unassigned --
floaternum 0 --subnetnum 5 --offset 1
(forward): running /opt/LSS/sbin/netconf_adm --action generate_host_
all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action generate_host_
all
dibc2-s00c03h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
(forward): running /opt/LSS/sbin/netconf_adm --action install_host_
all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action install_host_
all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
(forward): running rt4conf_adm --action add_service_address --
servicetype feph --poolnum 0 --subnetnum 5 --floaternum 0 --
offset 1 --nitype unassigned
(forward): running RTCONF_COMPLETE=1
(forward): running /opt/LSS/sbin/syncConfigDB -f -l
Command completed successfully.
(forward): running /opt/LSS/sbin/net4conf_adm --action add_service_
address --servicetype feph --poolnum 0 --nitype published --
floaternum 0 --subnetnum 5 --offset 1 --reuse

```

```
(forward): running /opt/LSS/sbin/net4conf_adm --action del_service_
    address --servicetype feph --poolnum 0 --nitype unassigned --
    floaternum 0 --subnetnum 5 --offset 1
(forward): running /opt/LSS/sbin/dnsconf_adm --action add_service_
    address4 --servicetype feph --poolnum 0 --floaternum 0 --
    subnetnum 5 --nitype published --offset 1
(forward): running DNS_COMPLETE=1
(forward): running /opt/LSS/sbin/netconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating service 1 configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
(forward): running /opt/LSS/sbin/netconf_adm --action install_host_
    all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action install_host_
    all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
(forward): running rt4conf_adm --action add_service_address --
    servicetype feph --poolnum 0 --subnetnum 5 --floaternum 0 --
    offset 1 --nitype published
(forward): running RTCONF_COMPLETE=1
(forward): running /opt/LSS/sbin/syncConfigDB -f -l
Command completed successfully.
(ssh_conf_adm): Running "/opt/LSS/sbin/sshconf_adm --action key_host_
    all"
dibc2-s00c03h0: generating SSH keys... done
dibc2-s00c01h4: generating SSH keys... done
dibc2-s00c02h4: generating SSH keys... done
dibc2-s00c04h0: generating SSH keys... done
dibc2-s00c15h0: aquiring SSH keys... done
(ssh_conf_adm): Running "/opt/LSS/sbin/sshconf_adm --action generate_
    member_instance --servicetype feph --poolnum 0"
dibc2-s00c01h4: generating SSH daemon configuration... done
dibc2-s00c02h4: generating SSH daemon configuration... done
(ssh_conf_adm): Running "/opt/LSS/sbin/sshconf_adm --action install_
    member_instance --servicetype feph --poolnum 0"
dibc2-s00c01h4: installing SSH daemon configuration... done
```

```

dibc2-s00c02h4: installing SSH daemon configuration... done
(ssh_conf_adm): Running "/opt/LSS/sbin/sshconf_adm --action control_
    member_instance --servicetype feph --poolnum 0 --command restart"
dibc2-s00c01h4: restart non root internal fixed ... done
dibc2-s00c01h4: restart root only internal fixed ... done
dibc2-s00c02h4: restart non root internal fixed ... done
dibc2-s00c02h4: restart root only internal fixed ... done
(ssh_conf_adm): Running sshconf_adm on OTHER_MI
dibc2-s00c01h4: generating SSH daemon configuration... done
dibc2-s00c02h4: generating SSH daemon configuration... done
"ip_adm -a add_floating_ip..." is successful. After testing, run "ip_
    adm -a commit".
Or you can backout via "ip_adm -a backout"
Executing: ip_adm -a commit
(checkmonitor): feph has a monitor type of rem
Running ip_adm
RCCavcmInhibitAdm: Request succeeded
(commit): running /opt/LSS/sbin/create_ht
Tue Mar 13 16:21:40 CST 2012 create_ht
Tue Mar 13 16:21:40 CST 2012 Saving backup files under /var/opt/lib/
    mtce/data
Tue Mar 13 16:21:40 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.data
Tue Mar 13 16:21:40 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.layout
Tue Mar 13 16:21:40 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.data
Tue Mar 13 16:21:40 CST 2012 Wrote new /var/opt/lib/mtce/1 data/mtce_
    tim.layout
Tue Mar 13 16:21:40 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.data
Tue Mar 13 16:21:40 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.layout
Tue Mar 13 16:21:40 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.data
Tue Mar 13 16:21:40 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.layout
Tue Mar 13 16:21:40 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    def_lib.ksh
(commit): running /opt/LSS/sbin/scdm_adm --action sync_config
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/netconf_adm --action
generate_host_all
dibc2-s00c04h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c03h0: generating network configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/svcconf_adm --action
generate_host_all
dibc2-s00c04h0: generating service configuration... done

```

```

dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c03h0: generating service configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64
  'export
PATH=/opt/LSS/sbin:/opt/LSS/bin:/opt/LU3P/sbin:/opt/LU3P/bin:/usr/
  /sbin:/usr/bin:/sbin:/bin:/usr/java/bin:/opt/LSS/sbin:/opt/LSS/
  bin ; /opt/LSS/sbin/create_ht'
Tue Mar 13 16:21:47 CST 2012 create_ht
Tue Mar 13 16:21:47 CST 2012 Saving backup files under /var/opt/lib/
  mtce/data
Tue Mar 13 16:21:47 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  host.data
Tue Mar 13 16:21:47 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  host.layout
Tue Mar 13 16:21:47 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  tim.data
Tue Mar 13 16:21:47 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  tim.layout
Tue Mar 13 16:21:47 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  srv.data
Tue Mar 13 16:21:47 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  srv.layout
Tue Mar 13 16:21:47 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  system.data
Tue Mar 13 16:21:47 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  system.layout
Tue Mar 13 16:21:47 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  def_lib.ksh
(commit): running /opt/LSS/sbin/scdm_adm --action commit_config
(commit): running clr_rcc_inhibit
"ip_adm -a commit" completed successfully.
Executing: ip_adm -a add_floating_ip -t feph -i 0 -s 11 -o 2620:0000:
  0060:401f:0000:0000:0000:0491 -n published
(checkmonitor): feph has a monitor type of rem
Running ip_adm
RCCavcmInhibitAdm: Request succeeded
(forward): running /opt/LSS/sbin/scdm_adm --action check_health
sorting metadata between MIs....
checking metadata between MIs....
done..
(forward): running rm -rf /var/opt/lib/scdt/backup
(forward): running /opt/LSS/sbin/scdm_adm --action backup_config
(forward): running /opt/LSS/sbin/net6conf_adm --action add_service_
  address --servicetype feph --poolnum 0 --
nitype unassigned --floaternum 0 --subnetnum 11 --address6 2620:0000:
  0060:401f:0000:0000:0000:0491
(forward): running /opt/LSS/sbin/netconf_adm --action generate_host_
  all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done

```

```

dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating service 1 configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
(forward): running /opt/LSS/sbin/net6conf_adm --action generate_host_
    all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/net6conf_adm --action install_host_
    all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/netconf_adm --action install_host_
    all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action install_host_
    all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
(forward): running rt6conf_adm --action add_service_address --
    servicetype feph --poolnum 0 --subnetnum 11 --floaternum 0 --
    address6 2620:0000:0060:401f:0000:0000:0491 --nitype
    unassigned
(forward): running RTCONF_COMPLETE=1
(forward): running /opt/LSS/sbin/syncConfigDB -f -l
Command completed successfully.
(forward): running /opt/LSS/sbin/net6conf_adm --action add_service_
    address --servicetype feph --poolnum 0 --nitype published --
    floaternum 0 --subnetnum 11 --address6 2620:0000:0060:401f:0000:
    0000:0000:0491 --reuse
(forward): running /opt/LSS/sbin/net6conf_adm --action del_service_
    address --servicetype feph --poolnum 0 --nitype unassigned --
    floaternum 0 --subnetnum 11 --address6 2620:0000:0060:401f:0000:
    0000:0000:0491
(forward): running /opt/LSS/sbin/dnsconf_adm --action add_service_
    address6 --servicetype feph --poolnum 0 --floaternum 0 --
    subnetnum 11 --nitype published --address6 2620:0000:0060:401f:
    0000:0000:0000:0491
(forward): running DNS_COMPLETE=1
(forward): running /opt/LSS/sbin/netconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done

```

```

dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action generate_host_all
dibc2-s00c03h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
(forward): running /opt/LSS/sbin/net6conf_adm --action generate_host_all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/net6conf_adm --action install_host_all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/netconf_adm --action install_host_all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action install_host_all
dibc2-s00c03h0: installing service 1 configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
(forward): running rt6conf_adm --action add_service_address --
servicetype feph --poolnum 0 --subnetnum 11 --floaternum 0 --
address6 2620:0000:0060:401f:0000:0000:0491 --nitype
published
(forward): running RTCONF_COMPLETE=1
(forward): running /opt/LSS/sbin/syncConfigDB -f -1
Command completed successfully.
(ssh_conf_adm): Running "/opt/LSS/sbin/sshconf_adm --action key_host_all"
dibc2-s00c03h0: generating SSH keys... done
dibc2-s00c01h4: generating SSH keys... done
dibc2-s00c02h4: generating SSH keys... done
dibc2-s00c04h0: generating SSH keys... done
dibc2-s00c15h0: aquiring SSH keys... done
(ssh_conf_adm): Running "/opt/LSS/sbin/sshconf_adm --action generate_member_instance --servicetype feph --poolnum 0"
dibc2-s00c01h4: generating SSH daemon configuration... done
dibc2-s00c02h4: generating SSH daemon configuration... done
(ssh_conf_adm): Running "/opt/LSS/sbin/sshconf_adm --action install_member_instance --servicetype feph --poolnum 0"
dibc2-s00c01h4: installing SSH daemon configuration... done
dibc2-s00c02h4: installing SSH daemon configuration... done
(ssh_conf_adm): Running "/opt/LSS/sbin/sshconf_adm --action control_member_instance --servicetype feph --poolnum 0 --command restart"

```

```

dibc2-s00c01h4: restart non root internal fixed ... done
dibc2-s00c01h4: restart root only internal fixed ... done
dibc2-s00c02h4: restart non root internal fixed ... done
dibc2-s00c02h4: restart root only internal fixed ... done
(ssh_conf_adm): Running sshconf_adm on OTHER_MI
dibc2-s00c01h4: generating SSH daemon configuration... done
dibc2-s00c02h4: generating SSH daemon configuration... done
"ip_adm -a add_floating_ip..." is successful. After testing, run "ip_
adm -a commit".
Or you can backout via "ip_adm -a backout"
Executing: ip_adm -a commit
(checkmonitor): rceph has a monitor type of rem
Running ip_adm
RCCavcmInhibitAdm: Request succeeded
(commit): running /opt/LSS/sbin/create_ht
Tue Mar 13 16:25:57 CST 2012 create_ht
Tue Mar 13 16:25:57 CST 2012 Saving backup files under /var/opt/lib/
mtce/data
Tue Mar 13 16:25:57 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
host.data
Tue Mar 13 16:25:57 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
host.layout
Tue Mar 13 16:25:57 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
tim.data
Tue Mar 13 16:25:57 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
tim.layout
Tue Mar 13 16:25:57 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
srv.data
Tue Mar 13 16:25:57 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
srv.layout
Tue Mar 13 16:25:57 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
system.data
Tue Mar 13 16:25:57 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
system.layout
Tue Mar 13 16:25:57 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
def_lib.ksh
(commit): running /opt/LSS/sbin/scdm_adm --action sync_config
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
LSS/sbin/netconf_adm --action
generate_host_all
dibc2-s00c04h0: generating network configuration... done
dibc2-s00c01h4: generating 1 network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c03h0: generating network configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
LSS/sbin/svcconf_adm --action
generate_host_all
dibc2-s00c04h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c03h0: generating service configuration... done

```

```
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64
  'export
PATH=/opt/LSS/sbin:/opt/LSS/bin:/opt/LU3P/sbin:/opt/LU3P/bin:/usr/
  sbin:/usr/bin:/sbin:/bin:/usr/java/bin:/opt/LSS/sbin:/opt/LSS/
  bin ; /opt/LSS/sbin/create_ht'
Tue Mar 13 16:26:04 CST 2012 create_ht
Tue Mar 13 16:26:04 CST 2012 Saving backup files under /var/opt/lib/
  mtce/data
Tue Mar 13 16:26:04 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  host.data
Tue Mar 13 16:26:04 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  host.layout
Tue Mar 13 16:26:04 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  tim.data
Tue Mar 13 16:26:04 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  tim.layout
Tue Mar 13 16:26:04 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  srv.data
Tue Mar 13 16:26:04 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  srv.layout
Tue Mar 13 16:26:04 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  system.data
Tue Mar 13 16:26:04 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  system.layout
Tue Mar 13 16:26:04 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
  def_lib.ksh
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
  LSS/sbin/net6conf_adm --action
generate_host_all
dibc2-s00c04h0: generating network configuration... done
dibc2-s00c03h0: generating network configuration... done
(commit): running /opt/LSS/sbin/scdm_adm --action commit_config
(commit): running clr_rcc_inhibit
"ip_adm -a commit" completed successfully.
fephSubnetCvt.ksh: Completed Successfully.
fephSubnetCvt.ksh Log: /var/opt/log/fephSubnetCvt/fephSubnetCvt.log
fephSubnetCvt.ksh ended 03/13/12 16:26.
```

---

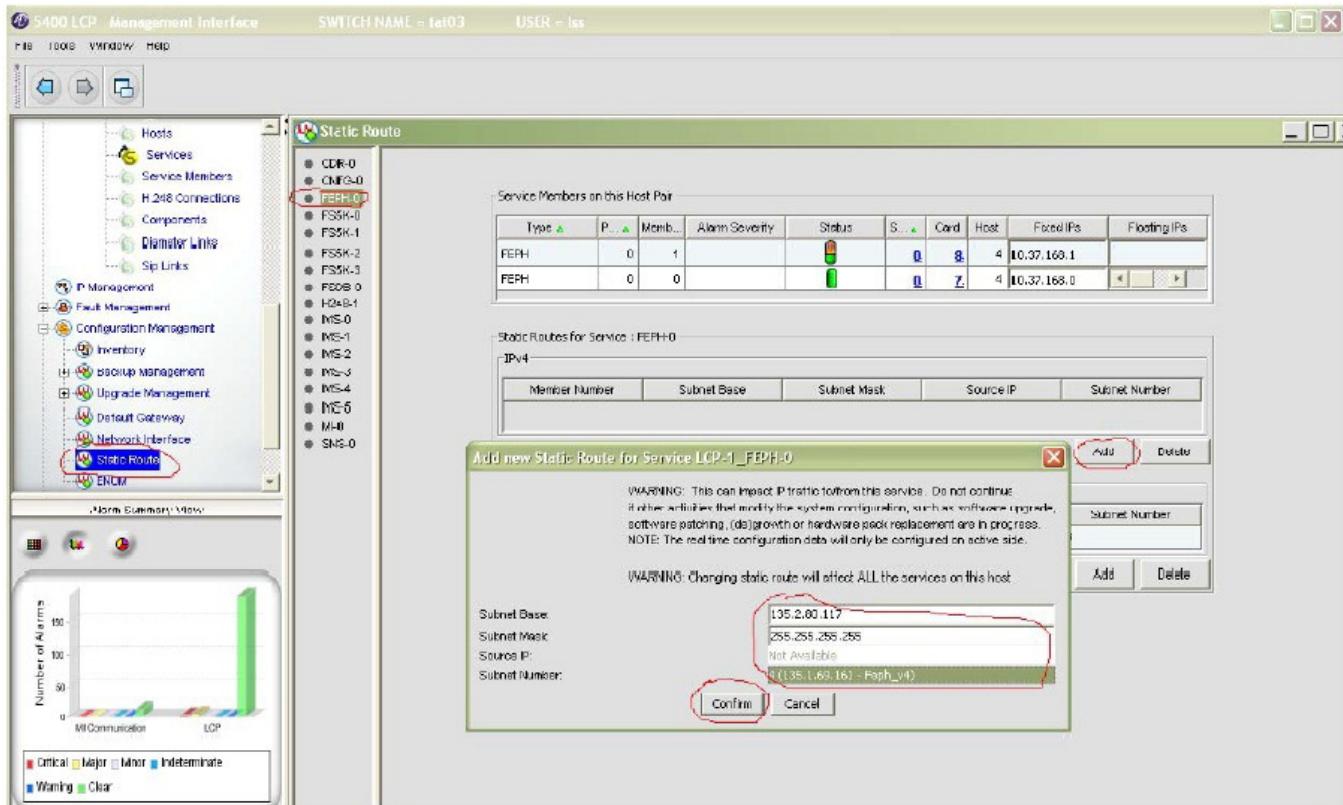
## 2 Add IPv4 and/or IPv6 static route for the new external access subnet.

## Manage services

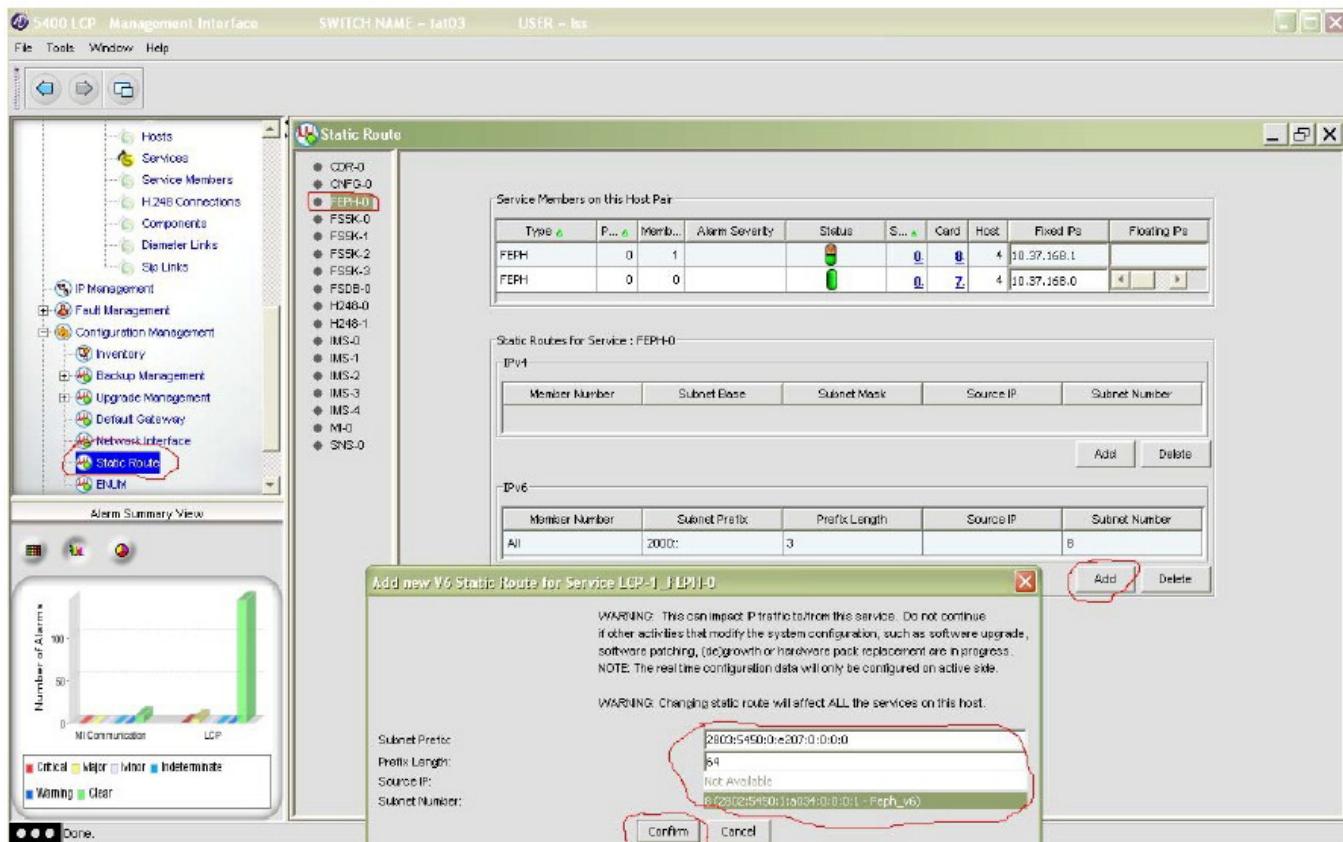
Support Multiple Access Network Subnets on FEPH

To convert one ordinary subnet to external access subnet

The following figure shows the process of adding IPv4 static route for the new subnet on FEPH.



The following figure shows the process of adding IPv6 static route for the new subnet on FEPH.



### 3 Enable FEPH service on the new external access subnet for IMS service.

For the detail procedure, see “To grow Signaling Firewall and FEPH on a new network” (p. 5-191).

E N D O F S T E P S

# To degrow one external access subnet

## Purpose

This topic describes the procedure to degrow one external access subnet.

## Before you begin

Before using fephSubnetCvt to perform FEPH subnet conversion, the system environment must be ready with the following:

- The state for all pairs of cards is InserviceActive/InserviceStbyHot.
- This tool can only be run in Active MI with root login, so it must be ensured that the “startMI” is run before doing conversion.
- FEPH service has been grown to the system.

**Note:** Before going through the following procedure, it is recommended that the **fephSubnetCvt -b** is run to backup the system configuration. If some failures are encountered during the following procedure, the **fephSubnetCvt -u i** is run to restore the network configuration that is backed up.

## Procedure

Perform the following procedure to degrow one external access subnet.

- 
- 1 Run fephSubnetCvt -d to delete the published IP from FEPH.

**Example:** The following is an example for deleting published IP from FEPH:

```
<dibc2-s00c03h0:root>/root/jli053:  
# fephSubnetCvt -d  
fephSubnetCvt.ksh: started 03/13/12 13:18  
Align RCC VMs  
RCCavcmInhibitAdm: Requested mode already set  
RCCavcmInhibitAdm: Requested mode already set  
Enabled MI switchover  
All RCC VM's are now aligned  
Delete IPv4 or IPv6 subnet to the FEPH Service (Enter 4, 6, or q to  
quit): 4  
IPv4 subnets currently assigned to FEPH:  
service type feph, pool number 0, floater number 0, IPv4 subnet  
number 2, NI type published, offset 5, IPv4 IP address  
10.84.22.197  
service type feph, pool number 0, floater number 0, IPv4 subnet  
number 5, NI type published, offset 1, IPv4 IP address  
10.84.22.225  
Enter IPv4 subnet number which you want to delete from FEPH: 5  
/opt/LSS/sbin/netconf_adm --action generate_host_all  
dibc2-s00c03h0: generating network configuration... done
```

```

dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
/opt/LSS/sbin/svcconf_adm --action generate_host_all
dibc2-s00c03h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
/opt/LSS/sbin/netconf_adm --action install_host_all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
/opt/LSS/sbin/svcconf_adm --action install_host_all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
/opt/LSS/sbin/syncConfigDB -f -l
Command completed successfully.
/opt/LSS/sbin/scdm_adm --action sync_config
/opt/LSS/sbin/scdm_adm --action commit_config
No backup key directory found. Skipping command.
No backup directory found. Skipping command.
Executing: ip_adm -a del_floating_ip -t feph -i 0 -s 5 -o 1
(checkmonitor): feph has a monitor type of rem
Running ip_adm
    RCCavcmInhibitAdm: Request succeeded
(forward): running /opt/LSS/sbin/scdm_adm --action check_health
sorting metadata between MIs....
checking metadata between MIs....
done..
(forward): running rm -rf /var/opt/lib/scdt/backup
(forward): running /opt/LSS/sbin/scdm_adm --action backup_config
(forward): running /opt/LSS/sbin/dnsconf_adm --action del_service_
    address4 --servicetype feph --poolnum 0 --floaternum 0 --
    subnetnum 5 --nitype unassigned --offset 1
(forward): running DNS_COMPLETE=1
(forward): running rt4conf_adm --action del_service_address --
    servicetype 1 feph --poolnum 0 --subnetnum 5 --floaternum 0 --
    offset 1 --nitype unassigned
(forward): running RTCONF_COMPLETE=1
(forward): running /opt/LSS/sbin/net4conf_adm --action del_service_
    address --servicetype feph --poolnum 0 --nitype unassigned --
    floaternum 0 --subnetnum 5 --offset 1
(forward): running /opt/LSS/sbin/netconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done

```

```

dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action generate_host_
    all
dibc2-s00c03h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
(forward): running /opt/LSS/sbin/netconf_adm --action install_host_
    all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action install_host_
    all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
(forward): running /opt/LSS/sbin/syncConfigDB -f -l
Command completed successfully.
"ip_adm -a del_floating_ip..." is successful. After testing, run "ip_
    adm -a commit".
Or you can backout via "ip_adm -a backout"
Executing: ip_adm -a commit
(checkmonitor): feph has a monitor type of rem
Running ip_adm
RCCavcmInhibitAdm: Request succeeded
(commit): running /opt/LSS/sbin/create_ht
Tue Mar 13 13:21:54 CST 2012 create_ht
Tue Mar 13 13:21:54 CST 2012 Saving backup files under /var/opt/lib/
    mtce/data
Tue Mar 13 13:21:54 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.data
Tue Mar 13 13:21:54 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.layout
Tue Mar 13 13:21:54 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.data
Tue Mar 13 13:21:54 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.layout
Tue Mar 13 13:21:54 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.data
Tue Mar 13 13:21:54 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.layout
Tue Mar 13 13:21:54 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.data
Tue Mar 13 13:21:54 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.layout
Tue Mar 13 13:21:54 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    def_lib.ksh
(commit): running /opt/LSS/sbin/scdm_adm --action sync_config

```

```
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/netconf_adm --action
generate_host_all
dibc2-s00c04h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c03h0: generating network configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/svcconf_adm --action
generate_host_all
dibc2-s00c04h0: generating service 1 configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c03h0: generating service configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64
    'export
PATH=/opt/LSS/sbin:/opt/LSS/bin:/opt/LU3P/sbin:/opt/LU3P/bin:/usr/
    sbin:/usr/bin:/sbin:/bin:/usr/java/bin:/opt/LSS/sbin:/opt/LSS/
    bin ; /opt/LSS/sbin/create_ht'
Tue Mar 13 13:22:01 CST 2012 create_ht
Tue Mar 13 13:22:01 CST 2012 Saving backup files under /var/opt/lib/
    mtce/data
Tue Mar 13 13:22:01 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.data
Tue Mar 13 13:22:01 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    host.layout
Tue Mar 13 13:22:01 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.data
Tue Mar 13 13:22:01 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    tim.layout
Tue Mar 13 13:22:01 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.data
Tue Mar 13 13:22:01 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    srv.layout
Tue Mar 13 13:22:01 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.data
Tue Mar 13 13:22:01 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.layout
Tue Mar 13 13:22:01 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    def_lib.ksh
(commit): running /opt/LSS/sbin/scdm_adm --action commit_config
(commit): running clr_rcc_inhibit
"ip_adm -a commit" completed successfully.
Success to delete subnet (subnet_number = 5) from FEPH service
IPv4 subnets currently assigned to FEPH:
service type feph, pool number 0, floater number 0, IPv4 subnet
    number 2, NI type published, offset 5, IPv4 IPaddress 10.84.22.197
Delete IPv4 or IPv6 subnet to the FEPH Service (Enter 4, 6, or q to
    quit): 6
IPv6 subnets currently assigned to FEPH:
service type feph, pool number 0, floater number 0, IPv6 subnet
    number 11, IPv6 IP address
```

```

2620:0000:0060:401f:0000:0000:0000:0491, NI type published
service type feph, pool number 0, floater number 0, IPv6 subnet
number 7, IPv6 IP address
2620:0:60:401F:0:0:0:417, NI type published
Enter IPv6 subnet number which you want to delete from FEPH: 11
/opt/LSS/sbin/netconf_adm --action generate_host_all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
/opt/LSS/sbin/svcconf_adm --action generate_host_all
dibc2-s00c03h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
/opt/LSS/sbin/netconf_adm --action install_host_all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
/opt/LSS/sbin/svcconf_adm --action install_host_all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
/opt/1 LSS/sbin/syncConfigDB -f -l
Command completed successfully.
/opt/LSS/sbin/scdm_adm --action sync_config
/opt/LSS/sbin/scdm_adm --action commit_config
No backup key directory found. Skipping command.
No backup directory found. Skipping command.
Executing: ip_adm -a del_floating_ip -t feph -i 0 -s 11 -o 2620:0000:
0060:401f:0000:0000:0000:0491
(checkmonitor): feph has a monitor type of rem
Running ip_adm
RCCavcmInhibitAdm: Request succeeded
(forward): running /opt/LSS/sbin/scdm_adm --action check_health
sorting metadata between MIs....
checking metadata between MIs....
done..
(forward): running rm -rf /var/opt/lib/scdt/backup
(forward): running /opt/LSS/sbin/scdm_adm --action backup_config
(forward): running /opt/LSS/sbin/dnsconf_adm --action del_service_
address6 --servicetype feph --poolnum 0 --floaternum 0 --
subnetnum 11 --nitype unassigned --address6 2620:0000:0060:401f:
0000:0000:0000:0491
(forward): running DNS_COMPLETE=1

```

```
(forward): running rt6conf_adm --action del_service_address --
servicetype feph --poolnum 0 --subnetnum 11 --floaternum 0 --
address6 2620:0000:0060:401f:0000:0000:0491 --nitype
unassigned
(forward): running RTCONF_COMPLETE=1
(forward): running /opt/LSS/sbin/net6conf_adm --action del_service_
address --servicetype feph --poolnum 0 --
nitype unassigned --floaternum 0 --subnetnum 11 --address6 2620:0000:
0060:401f:0000:0000:0491
(forward): running /opt/LSS/sbin/netconf_adm --action generate_host_
all
dibc2-s00c03h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c04h0: generating network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action generate_host_
all
dibc2-s00c03h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c04h0: generating service configuration... done
(forward): running /opt/LSS/sbin/netconf_adm --action install_host_
all
dibc2-s00c03h0: installing network configuration... done
dibc2-s00c01h4: installing network configuration... done
dibc2-s00c02h4: installing network configuration... done
dibc2-s00c04h0: installing network configuration... done
(forward): running /opt/LSS/sbin/svcconf_adm --action install_host_
all
dibc2-s00c03h0: installing service configuration... done
dibc2-s00c01h4: installing service configuration... done
dibc2-s00c02h4: installing service configuration... done
dibc2-s00c04h0: installing service configuration... done
(forward): running /opt/LSS/sbin/syncConfigDB -f -1
Command completed successfully.
"ip_adm -a del_floating_ip..." is successful. After testing, run "ip_
adm -a commit".
Or you can backout via "ip_adm -a backout"
Executing: ip_adm -a commit
(checkmonitor): feph has a monitor type of rem
Running ip_adm
RCCavcmInhibitAdm: Request succeeded
(commit): running /opt/LSS/sbin/create_ht
Tue Mar 13 13:26:43 CST 2012 create_ht
Tue Mar 13 13:26:43 CST 2012 Saving backup files under 1 /var/opt/
lib/mtce/data
Tue Mar 13 13:26:43 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
host.data
Tue Mar 13 13:26:43 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
host.layout
```

```

Tue Mar 13 13:26:43 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
tim.data
Tue Mar 13 13:26:43 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
tim.layout
Tue Mar 13 13:26:43 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
srv.data
Tue Mar 13 13:26:43 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
srv.layout
Tue Mar 13 13:26:43 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
system.data
Tue Mar 13 13:26:43 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
system.layout
Tue Mar 13 13:26:43 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
def_lib.ksh
(commit): running /opt/LSS/sbin/scdm_adm --action sync_config
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
LSS/sbin/netconf_adm --action
generate_host_all
dibc2-s00c04h0: generating network configuration... done
dibc2-s00c01h4: generating network configuration... done
dibc2-s00c02h4: generating network configuration... done
dibc2-s00c03h0: generating network configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
LSS/sbin/svcconf_adm --action
generate_host_all
dibc2-s00c04h0: generating service configuration... done
dibc2-s00c01h4: generating service configuration... done
dibc2-s00c02h4: generating service configuration... done
dibc2-s00c03h0: generating service configuration... done
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64
'export
PATH=/opt/LSS/sbin:/opt/LSS/bin:/opt/LU3P/sbin:/opt/LU3P/bin:/usr/
sbin:/usr/bin:/sbin:/bin:/usr/java/bin:/opt/LSS/sbin:/opt/LSS/
bin ; /opt/LSS/sbin/create_ht'
Tue Mar 13 13:26:50 CST 2012 create_ht
Tue Mar 13 13:26:50 CST 2012 Saving backup files under /var/opt/lib/
mtce/data
Tue Mar 13 13:26:50 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
host.data
Tue Mar 13 13:26:50 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
host.layout
Tue Mar 13 13:26:50 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
tim.data
Tue Mar 13 13:26:50 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
tim.layout
Tue Mar 13 13:26:50 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
srv.data
Tue Mar 13 13:26:50 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
srv.layout
Tue Mar 13 13:26:50 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
system.data

```

```
Tue Mar 13 13:26:50 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    system.layout
Tue Mar 13 13:26:50 CST 2012 Wrote new /var/opt/lib/mtce/data/mtce_
    def_lib.ksh
(commit): running /opt/LSS/sbin/remote_shell root 169.254.64.64 /opt/
    LSS/sbin/net6conf_adm --action
generate_host_all
dibc2-s00c04h0: generating network configuration... done
dibc2-s00c03h0: generating network configuration... done
(commit): running /opt/LSS/sbin/scdm_adm --action commit_config
(commit): running clr_rcc_inhibit
"ip_adm -a commit" completed successfully.
Success to delete subnet (subnet_number = 11) from FEPH service
IPv6 subnets currently assigned to FEPH:
service type feph, pool number 0, floater number 0, IPv6 subnet
    number 7, IPv6 IP address
2620:0:60:401F:0:0:0:417, NI type published
49
Delete IPv4 or IPv6 subnet to the FEPH Service (Enter 4, 6, or q to
    quit): q
fehpSubnetCvt.ksh: Completed Successfully.
fehpSubnetCvt.ksh Log: /var/opt/log/fehpSubnetCvt/fehpSubnetCvt.log
fehpSubnetCvt.ksh ended 03/13/12 13:38.
```

END OF STEPS

# 6 Translations

## Overview

### Purpose

This chapter describes translations that are specific to the 5450 IP Session Control (ISC) application.

### Contents

|                              |            |
|------------------------------|------------|
| <b>BGCF Translations</b>     | <b>6-2</b> |
| BGCF translations            | 6-3        |
| BGCF CIC dialing prefix      | 6-4        |
| BGCF per-carrier translation | 6-5        |
| BGCF sample translations     | 6-6        |

# BGCF Translations

## Overview

### Purpose

This section describes BGCF Translations.

### Contents

|                              |     |
|------------------------------|-----|
| BGCF translations            | 6-3 |
| BGCF CIC dialing prefix      | 6-4 |
| BGCF per-carrier translation | 6-5 |
| BGCF sample translations     | 6-6 |

# BGCF translations

## Need for BGCF translations

BGCF translations are required for the following tasks:

- To send outgoing calls that are known to be off-net (PSTN) to the MGCF.
- To send outgoing calls that may be either on-net or off-net (PSTN) to the Interrogating Call Session Control Function I-CSCF before the Media Gateway Control Function (MGCF).
- To match originating calls that contain a dialed or pre-subscribed CIC.

# BGCF CIC dialing prefix

## CIC dialing prefix

One entry per system is available to recognize a dialed CIC string. The dialed CIC string is defined at **IMS ->Parameters/Timers -> NGSS Parameters**. This entry is only valid when the CIC is four digits in length.

### Setting BGCF CIC Dialing Prefix

The following table shows the value of the **BGCF CIC Dialing Prefix** for customers:

| Customer                  | BGCF CIC Dialing Prefix value |
|---------------------------|-------------------------------|
| US Equal Access customers | 101                           |
| Other customers           | blank                         |

# BGCF per-carrier translation

## Calling Party Number CIC

A calling Party Number CIC match is required for any system that can signal a pre-subscribed carrier to the BGCF.

## US Equal Access customers

The following options are available for US Equal Access customers:

- Provide a Calling Party Number CIC match for each 4-digit CIC that may be dialed or pre-subscribed. Calls may be sent to differing targets according to the carrier.
- A wildcard CIC can be used to represent all CICs. The wildcard CIC is the value '&'.

If a wildcard CIC is used along with specific 4-digit CICs, the wildcard has the lowest precedence (for example, it is default).

## Customers using IN Query mode

For customers using IN Query mode:

- No per-carrier translation in the BGCF is required.
- Provide called number entries to match Carrier Select Calls (for example, 10& and 16&).

## Customers using digit analysis mode 1

For customers using digit analysis mode 1:

- Provide one Calling party number CIC match using a wildcard CIC of &.
- Provide called number entries to match Carrier Select Calls (for example, 18&).

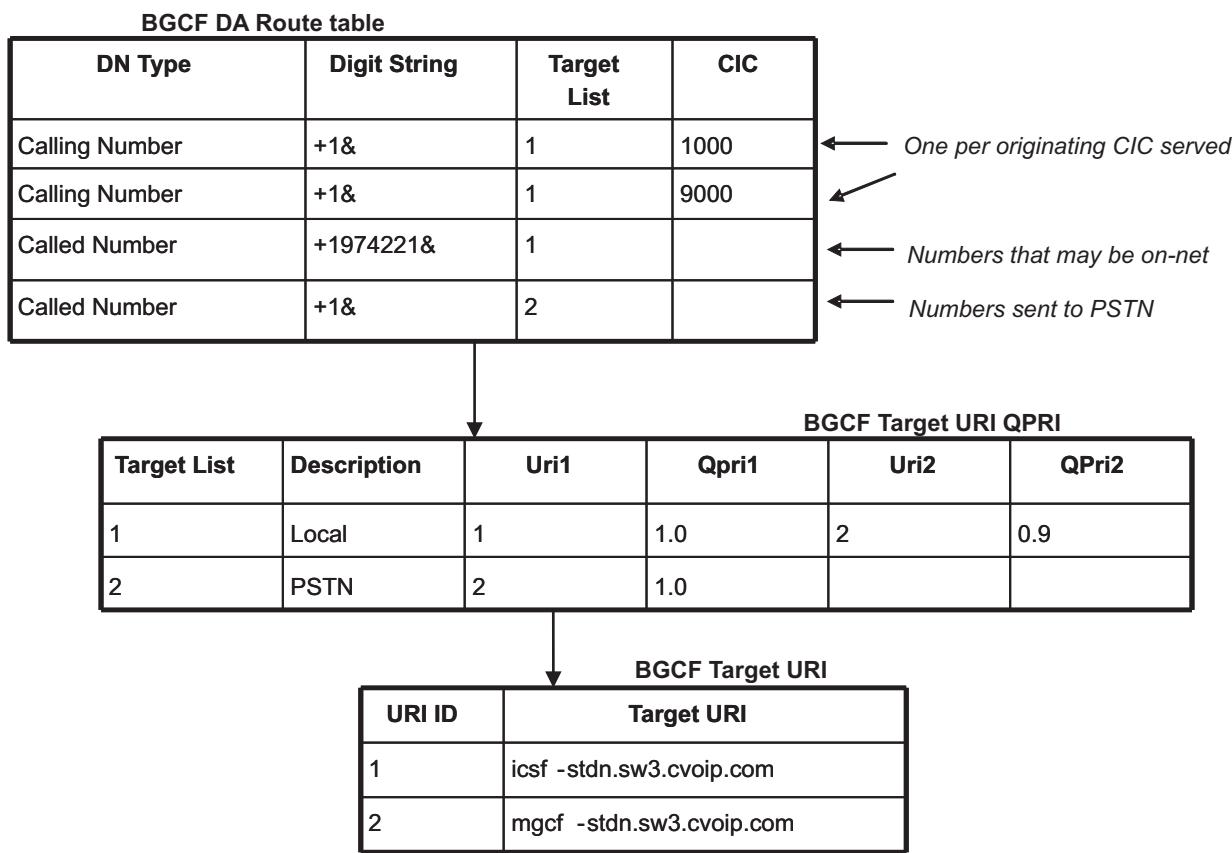
# BGCF sample translations

## Purpose

This topic shows an example of BGCF translations and explains the purpose and use of the translations.

## BGCF DA Route example

The following figure shows an example of BGCF translations.



## BGCF DA Route table purpose

The translations from the example BGCF DA Route table serve the following purposes:

- Identify Target List for calls originating from country code 1 with a dialed or pre-subscribed carrier ID (CIC) of 1000 (see “[Notes](#)” (p. 6-7), note 1).
- Identify Target List for calls originating from country code 1 with a dialed or pre-subscribed carrier ID (CIC) of 9000 (see “[Notes](#)” (p. 6-7), note 1).

- Identify Target List for calls destined to country code 1, NPA=974, NXX=221 that may either be on-net or off-net (PSTN) (see “[Notes](#)” (p. 6-7), note 2).
- Identify Target List for calls destined to country code 1 that are off-net (PSTN).

The table entries are made under:

- “IMS -> IMS Components -> BGCF Tables -> BGCF DA Route Table”

### BGCF Target URI QPRI table

The BGCF Target URI QPRI table in the following figure shows sample BGCF Route translations pointed to by the DA Route table (Target List). For each target, there is a list of URIs that the call will be offered to, from highest to lowest priority (for example, Qpri1 and Qpri2).

- Calls that may be on-net should be offered to the I-CSCF before any MGCF (see “[Notes](#)” (p. 6-7), notes 2, 3, and 4).
- Calls that are known to be off-net should be offered immediately to the MGCF (see “[Notes](#)” (p. 6-7), note 3).

### BGCF Target URI table

The BGCF Target URI table in the following figure shows sample BGCF Target URI translations that convert a Target URI given in the BGCF Target URL QPRI table to an actual URI.

### Notes

The following notes apply for the sample translations:

1. The per-carrier calling number translation is required for each carrier prefixed call reached either by pre-subscription (for example, CIC=parameter) or dial code (for example, 101XXXX) dial-around.
2. The target list should contain I-CSCF as the highest priority URI if the system should attempt on-net completion of pre-subscribed carrier calls.
3. The target list must contain one or more entries for MGCF to access the PSTN.
4. If the subscriber uses dial-around for an on-net destination (for example, 101XXXX 1 NPA NXX XXXX) the call will always be routed to the MGCF.
5. You can enter the digit string with or without the “+” sign in the **Value** field. However, routing remains the same.

### BGCF release codes for use with CTS application server

The IMS *BGCF Release Code* table lists SIP response codes that are to be treated as “final.” When a “final” code is received by the BGCF, there will be no advance to the next target URI.

The minimum, recommended, and conditional “BGCF release code” settings for use with the Converged Telephony Server (CTS) are shown in the following table. The ranges shown are inclusive.

| Category  | SIP response codes   |
|---|--|
| Minimum Set (per RFC 3261)                      | 300-302, 305, 380<br>400-403, 405-407, 410, 413-416, 420, 421,<br>423, 480-488, 491, 493<br>500-502, 504, 505, 513<br>600, 603, 604, 606 |
| Additional values recommended by Alcatel-Lucent | 409, 411, 417, 422, 433, 489, 494<br>580<br>688  |
| Conditional                                     | 404  |

**Notes:**

1. A maximum of 60 SIP response codes may be listed as “Final”.
2. SIP responses 408 and 503 should not be listed in the Release Code table.
3. SIP response 404 must be omitted from the list of final responses if the “No Enum” option is used. This entry is normally handled during base system configuration.





# Part III: Service policy decision function (SPDF) configuration

## Overview

### Purpose

This documentation part provides procedures to perform OAM&P tasks.

### Contents

|  |     |
|--|-----|
| <a href="#">Chapter 7, Manage system configuration</a> | 7-1 |
|--|-----|



# 7 Manage system configuration

## Overview

### Purpose

This chapter provides the procedures to configure the Service Policy Decision Function (SPDF).

### Contents

|                                      |             |
|--------------------------------------|-------------|
| <b>3GPP2 SBBC</b>                    | <b>7-2</b>  |
| To provision a Subscriber Tier table | 7-3         |
| To provision an IP Filter table      | 7-6         |
| To provision a Rule Name table       | 7-11        |
| To provision a PCC Rule table        | 7-14        |
| To provision a Rule Name List table  | 7-20        |
| To provision a Policy Selector Table | 7-24        |
| <b>TISPAN RACS</b>                   | <b>7-28</b> |
| To add an H.248 Device Server        | 7-29        |
| To provision an H.248-controlled BGW | 7-32        |
| To provision a DSCP Profile table    | 7-36        |

# 3GPP2 SBBC

## Overview

### Purpose

This section provides the task flow to configure 3GPP2 SBBC and procedures that are specific to 3GPP2 SBBC configuration.

### Contents

|                                      |      |
|--------------------------------------|------|
| To provision a Subscriber Tier table | 7-3  |
| To provision an IP Filter table      | 7-6  |
| To provision a Rule Name table       | 7-11 |
| To provision a PCC Rule table        | 7-14 |
| To provision a Rule Name List table  | 7-20 |
| To provision a Policy Selector Table | 7-24 |

# To provision a Subscriber Tier table

## Purpose

This procedure is used to provision a Subscriber Tier table.

## Steps to provision a Subscriber Tier table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **PDF Tables**.

**Result:** The **PDF Tables** window is displayed.

- 2 In the left pane, expand the **Subscriber Tier** folder.

**Result:** The Subscriber Tier tables are displayed under the folder in the left pane.

If the folder is empty, add a Subscriber Tier table.

Perform the following steps in the **PDF Tables** window to add, rename, or delete a Subscriber Tier table :

| If you want to ...              | then ...   |
|---------------------------------|--|
| add a Subscriber Tier table,    | <ol style="list-style-type: none"><li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add Subscriber Tier table</b> window is displayed.</li><li>From the <b>Table Number</b> list, select the table number.</li><li>In the <b>Table Name</b> box, type a descriptive table name.</li><li>Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |
| rename a Subscriber Tier table, | <ol style="list-style-type: none"><li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename Subscriber Tier table</b> window is displayed.</li><li>In the <b>Table Name</b> box, type a new table name.</li><li>Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p>  |

| If you want to ...              | then ...   |
|---------------------------------|--|
| delete a Subscriber Tier table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Subscriber Tier table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the Subscriber Tier table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

**Note:** A Subscriber Tier table must have at least one profile and can hold up to 20 profiles.

- 4** Perform the following steps at the **PDF Tables** window to add, modify, or delete the Subscriber Tier table profiles:

| If you want to ...                         | then ...   |
|--|--|
| add the Subscriber Tier table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Subscriber Tier Attributes</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a Subscriber Tier table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Subscriber Tier Attributes</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                         | then ...   |
|--|--|
| delete a Subscriber Tier table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more table profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter                   | Provisioning                                     |
|-----------------------------|--|
| <b>Subscriber Tier ID</b>   | Select a unique ID for the Subscriber Tier.      |
| <b>Subscriber Tier Name</b> | Type a descriptive name for the Subscriber Tier. |

6 Click **OK**.

**Result:** The Subscriber Tier table attributes are provisioned successfully.

END OF STEPS

# To provision an IP Filter table

## Purpose

This procedure is used to provision an IP Filter table.

## Steps to provision an IP Filter table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **PDF Tables**.

**Result:** The **PDF Tables** window is displayed.

- 2 In the left pane, expand the **IP Filter** folder.

**Result:** The IP Filter tables are listed under the folder in the left pane.

If the folder is empty, add an IP Filter table.

Perform the following steps in the **PDF Tables** window to add, rename, or delete an IP Filter table :

| If you want to ...         | then ...  |
|----------------------------|---|
| add an IP Filter table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add IP Filter table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename an IP Filter table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename IP Filter table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |

| If you want to ...         | then ...  |
|----------------------------|---|
| delete an IP Filter table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an IP Filter table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the IP Filter table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

**Note:** A maximum of 200 entries can be added in the IP Filter Table

- 4 Perform the following steps at the **PDF Tables** window to add, modify, or delete the IP Filter table attributes:

| If you want to ...                    | then ...  |
|---------------------------------------|---|
| add the IP Filter table attributes,   | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The IP Filter window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify an IP Filter table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The IP Filter window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                    | then ...  |
|---------------------------------------|---|
| delete an IP Filter table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

**5** Provision the following parameters:

| Parameter             | Provisioning   |
|-----------------------|--|
| <b>IP Filter ID</b>   | Select a unique ID for the IP Filter   |
| <b>IP Filter Name</b> | Type a descriptive name for the IP filter  |
| <b>Direction</b>      | <p>Select the direction applied to the IP Filter</p> <p>The available options:</p> <ul style="list-style-type: none"> <li>• In</li> <li>• Out</li> </ul> <p>Flows with a direction of <b>in</b> are uplink flows.</p> <p>Flows with a direction of <b>out</b> are downlink flows.</p>                      |
| <b>IP type</b>        | <p>This field defines the IP type used for this filter. This field is unavailable. Currently, only IPv4 is supported.</p>  |
| <b>Source IP</b>      | <p>Type the source IP address of the flow.</p> <p>If the direction is “out”, this IP address is used as the IP Address of the UE. If the direction is “in”, then this IP address is used as the IP address that the UE is trying to reach.</p> <p>The valid values are 000-255.000-255.000-255.000-255</p> |

| Parameter                  | Provisioning  |
|----------------------------|---|
| <b>Source Netmask</b>      | <p>Type the netmask used to reduce the source network. Enter the number of binary digits that are used to designate the network.</p> <p>For example, the binary form of 255.255.255.0 is 11111111 11111111 11111111 00000000, the first 24 digits are used to designate the network, so type 24 here.</p> <p>If you want to allow any IP addresses, type 0.0.0.0 in the <b>Source IP</b> field and 0 in the <b>Source Netmask</b> fields. Values range from 0 to 32.</p>  |
| <b>Source Port</b>         | <p>Type the source port to be used</p> <p>Enter a String of 0 - 32 alphanumeric characters. Valid values are a-z A-Z 0-9 * # . , - + ' ~ ` ! @ \$ % ^ : ; = ( ) { } [ ] ? " ' &amp; &lt;&gt; / _   \</p> <p>This field supports three different formats:</p> <ul style="list-style-type: none"> <li>• a single port number (for example, 100)</li> <li>• a comma-separated port list (for example, 100,200,300)</li> <li>• a range of port (for example, 100-200).</li> </ul> <p>If you want to allow all the ports to be used, leave this field blank.</p> |
| <b>Protocol</b>            | Select the protocol allowed by the filter. If <b>IP</b> is selected, then any protocol is allowed.  |
| <b>Destination IP</b>      | <p>Type the destination IP address of the flow.</p> <p>If the direction is “in” this is the IP Address of the UE. If the direction is “out” then this is the IP address that the UE is trying to reach.</p>   |
| <b>Destination Netmask</b> | Type the destination netmask (used to reduce the source network).   |

| Parameter               | Provisioning  |
|-------------------------|---|
| <b>Destination Port</b> | <p>Type the destination port to be used.</p> <p>This field supports three different formats:</p> <ul style="list-style-type: none"> <li>• a single port number (for example, 100)</li> <li>• a comma-separated port list (for example, 100,200,300)</li> <li>• a range of port (for example, 100-200).</li> </ul> <p>If you want to allow all the ports to be used, leave this field blank.</p> |

**6** Click OK.

**Result:** The IP Filter table attributes are provisioned successfully.

END OF STEPS

# To provision a Rule Name table

## Purpose

This procedure is used to add, modify or delete the Rule Name table.

The Rule Name table stores the Rule Names that are used to form the charging rule-related AVPs for the Ty interface.

## Steps to provision a Rule Name table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → IMS Components → PDF Tables**.

**Result:** The **PDF Tables** window is displayed.

- 2 In the left pane, expand the **Rule Name** folder.

**Result:** The Rule Name tables are displayed under the folder in the left pane.

If the folder is empty, add a Rule Name table.

Perform the following steps in the **PDF Tables** window to add, rename, or delete a Rule Name table:

| If you want to ...     | then ...  |
|------------------------|---|
| add a Rule Name table, | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add Rule Name table</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |

| If you want to ...        | then ...  |
|---------------------------|---|
| rename a Rule Name table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename Rule Name table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a Rule Name table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Rule Name table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>                  |

- 3 Double-click the table to open the list of profiles defined for the table.  
Add the Rule Name table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.
- 4 Perform the following steps at the **PDF Tables** window to add, modify, or delete the Rule Name table attributes:

| If you want to ...                   | then ...   |
|--------------------------------------|--|
| add the Rule Name table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Rule Name</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| modify a Rule Name table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Rule Name</b> window is displayed.</li> <li>Modify the <b>Name</b> field. See <a href="#">Step 5</a>.</li> </ol> <p><i>End of steps</i></p>      |

| If you want to ...                   | then ...  |
|--------------------------------------|---|
| delete a Rule Name table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more table attributes that you want to delete.<br/>To select multiple rows, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes → Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

**5** Provision the following parameters:

| Parameter   | Provisioning  |
|-------------|---|
| <b>ID</b>   | Select a unique ID for the Rule Name  |
| <b>Type</b> | <p>Select the type of the rule name.<br/>The following are the available rule types:</p> <ul style="list-style-type: none"> <li>• AF Modification PCC Rule</li> <li>• Non-AF Modification PCC Rule</li> <li>• PEP Predefined Base Rule</li> <li>• PEP Predefined Rule</li> <li>• Session Initialization PCC Rule</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• If a PCC Rule is selected, the characteristics of the PCC rule must be defined in the PCC Rule table.</li> <li>• PEP Predefined Rule and PEP Predefined Base Rule are predefined in AGW</li> </ul> <p>The maximum count for each rule is:</p> <ul style="list-style-type: none"> <li>• 100 for PEP Predefined Rule and PCC Rule (including all three types)</li> <li>• 50 for PEP Predefined Base Rule.</li> </ul> |
| <b>Name</b> | Type a descriptive name for the rule.   |

**6** Click **OK**.

**Result:** The Rule Name table attributes are provisioned successfully.

END OF STEPS

# To provision a PCC Rule table

## Purpose

This procedure is used to provision a Policy and Charging Control (PCC) Rule table.

The PCC Rule table stores the PCC Rules that are used to form the charging rule related AVPs for the Ty interface

## Steps to provision a PCC Rule table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **PDF Tables**.

**Result:** The **PDF Table** window is displayed.

- 2 In the left pane, expand the **PCC Rule** folder.

**Result:** The PCC Rule tables are listed under the folder in the left pane.

If the folder is empty, add a PCC Rule table.

Perform the following steps in the **PCC Rule** window to add, rename, or delete a PCC Rule table :

| If you want to ...    | then ...  |
|-----------------------|---|
| add a PCC Rule table, | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add PCC Rule table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.<br/><i>End of steps</i></li> </ol> |

| If you want to ...       | then ...   |
|--------------------------|--|
| rename a PCC Rule table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename PCC Rule table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a PCC Rule table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a PCC Rule table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>                  |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the PCC Rule table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **PCC Rule** window to add, modify, or delete the PCC Rule table attributes:

| If you want to ...                 | then ...  |
|------------------------------------|---|
| add the PCC Rule table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>PCC Rule</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                  | then ...  |
|-------------------------------------|---|
| modify a PCC Rule table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>PCC Rule</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a PCC Rule table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>        |

**5** Provision the following parameters:

| Parameter          | Provisioning  |
|--------------------|---|
| PCC Rule Type      | <p>select a rule type.</p> <p>The following are the available options:</p> <ul style="list-style-type: none"> <li>• AF Modification</li> <li>• Non-AF Modification</li> <li>• Session Initialization</li> </ul> <p><b>Note:</b></p> <p>When AF Modification is selected, the following parameters are unavailable:</p> <ul style="list-style-type: none"> <li>• Authorized Uplink Band Width (kbps)</li> <li>• Authorized Downlink Band Width (kbps)</li> <li>• Uplink IP Filter</li> <li>• Downlink IP Filter</li> <li>• Flow Status</li> <li>• QoS Class Identifier</li> </ul> <p>When <b>Non-AF Modification</b> is selected, the following parameters are unavailable:</p> <ul style="list-style-type: none"> <li>• Authorized Uplink Band Width (kbps)</li> <li>• Authorized Downlink Band Width (kbps)</li> <li>• Qos Class Identifier</li> </ul> |
| PCC Rule Name      | Select a PCC Rule name.   |
| Precedence         | <p>Type the precedence of the PCC Rule.</p> <p>This parameter corresponds to the Precedence AVP in Charging-Rule-Definition AVP.</p> <p>The Precedence AVP defines the precedence of a PCC rule in case of overlapping PCC rules.</p> <p>A PCC rule with the precedence AVP with lower value takes the priority over a PCC rule with the Precedence AVP with higher value.</p> <p>The Precedence AVP is also used to indicate the valuation precedence of the TFT packet filters.</p>   |
| Service Identifier | <p>Type the service identifier of the PCC rule.</p> <p>This field corresponds to the Service-Identifier AVP.</p> <p>This field identifies the service or service component related to the service data flow in a PCC rule.</p>  |

| Parameter                                  | Provisioning   |
|--|--|
| <b>Rating Group</b>                        | <p>Type the value of the rating group of the PCC rule.</p> <p>This field corresponds to the Rating-Group AVP.</p> <p>This field identifies the charging key for the PCC rule used for rating purposes.</p>   |
| <b>Authorized Uplink BandWidth(kpbs)</b>   | Type the Authorized Uplink Bandwidth.  |
| <b>Authorized Downlink BandWidth(kpbs)</b> | Type the Authorized Downlink Bandwidth.  |
| <b>Uplink IP Filter</b> and                | <p>Select uplink IP Filter (Provisioned in IP Filters table) for the corresponding PCC Rule.</p> <p>The filters are matched against the flowing descriptions in Ty messages. Only the matching rules are sent to AGW.</p>  |
| <b>Downlink IP Filter</b>                  | <p>Select the downlink IP Filter as provisioned in IP Filter table for the corresponding PCC Rule.</p> <p>The filters are matched against the flowing descriptions in Ty messages. Only the matching rules are sent to AGW.</p>  |
| <b>Flow Status</b>                         | <p>Select the flow status of the PCC Rule.</p> <p>This field corresponds to the Flow-Status AVP.</p> <p>The following are the available options:</p> <ul style="list-style-type: none"> <li>• Disabled</li> <li>• Downlink Enabled</li> <li>• Enabled</li> <li>• Uplink Enabled</li> </ul>   |
| <b>QoS Class Identifier</b>                | <p>Select the QoS Class Identifier.</p> <p>This field lists from Traffic Class 1 to Traffic Class 9.</p>   |
| <b>Reporting Level</b>                     | <p>Select the reporting level for the PCC rule.</p> <p>The following are the available options:</p> <ul style="list-style-type: none"> <li>• Rating Group Level[1]</li> <li>• Service Identifier Level[1]</li> </ul> <p>This field corresponds to the Reporting-Level AVP.</p> <p>The Reporting-Level AVP is of type Enumerated, and defines on what level the AGW reports the usage for the related PCC rule.</p> |

| Parameter                      | Provisioning  |
|--------------------------------|---|
| <b>Metering Method</b>         | <p>Select the Metering Method.</p> <p>The following are the available options:</p> <ul style="list-style-type: none"> <li>• Volume</li> <li>• Duration</li> <li>• Duration and Volume</li> </ul> <p>This field corresponds to the Metering-Method AVP.</p> <p>The Metering-Method AVP (AVP code 1007) is of type Enumerated, and defines what parameters shall be metered for offline charging.</p> |
| <b>Offline Charging Option</b> | <p>Select this option to enable the offline charging interface from the AGW for the associated charging rule.</p> <p>The absence of this AVP indicates that the default configuration is used.</p>  |
| <b>Online Charging Option</b>  | <p>Select this option to enable the online charging interface from the AGW for the associated charging rule.</p> <p>The absence of this AVP indicates that the default configuration is used.</p>   |

For more information on the parameters, see the topic **PCC Rule** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

**6** Click **OK**.

**Result:** The PCC Rule table attributes are provisioned successfully.

END OF STEPS

# To provision a Rule Name List table

## Purpose

This procedure is used to provision a Rule Name List table.

## Steps to provision a Rule Name List table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **PDF Tables**.

**Result:** The **PDF** window is displayed.

- 2 In the left pane, expand the **Rule Name List** folder.

**Result:** The Rule Name List tables are listed under the folder in the left pane.

If the folder is empty, add a Rule Name List table.

Perform the following steps in the **PDF Tables** window to add, rename, or delete a Rule Name List table :

| If you want to ...             | then ...  |
|--------------------------------|---|
| add a Rule Name List table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add Rule Name List table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.<br/><i>End of steps</i></li> </ol> |
| rename a Rule Name List table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename Rule Name List table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.<br/><i>End of steps</i></li> </ol>  |

| If you want to ...             | then ...  |
|--------------------------------|---|
| delete a Rule Name List table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Rule Name List table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the Rule Name List table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **PDF Tables** window to add, modify, or delete the Rule Name List table attributes:

| If you want to ...                        | then ...  |
|---|---|
| add the Rule Name List table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Rule Name List</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a Rule Name List table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Rule Name List</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                        | then ...  |
|---|---|
| delete a Rule Name List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

**5** Provision the following parameters:

| Parameter                | Provisioning  |
|--------------------------|---|
| <b>Rule Name List ID</b> | Select a unique ID for the Rule Name List.  |
| <b>Description</b>       | Type a descriptive name for the Rule Name List.   |
| <b>Type</b>              | Select the Rule Name List type<br>The available options are as follows: <ul style="list-style-type: none"> <li>Session Initialization PCC Rule</li> <li>Non-AF Modification PCC Rule</li> <li>PEP Predefined Rule</li> <li>PEP Predefined Base Rule</li> </ul>  |
| <b>Rule Name</b>         | One or more Rule Names can be associated to a Rule Name List.<br><br>Perform the following steps to associate a rule name to the rule name list: <ol style="list-style-type: none"> <li>Click <b>Add</b>.<br/><b>Result:</b> The <b>Add Rule Name</b> dialog is displayed</li> <li>Select the rule name and click <b>OK</b>.<br/><b>Result:</b> The selected rule name is displayed in the Rule name list box.</li> </ol> |

For more information on the parameters, see the topic **Rule Name List** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 
- 6 Click OK.

**Result:** The Rule Name List table attributes are provisioned successfully.

END OF STEPS

---

# To provision a Policy Selector Table

## Purpose

This procedure is used to provision a Policy Selector table.

## Before you begin

Perform the following:

- Provision a Subscriber Tier table.  
See “[To provision a Subscriber Tier table](#)” (p. 7-3)
- Provision a PEP Predefined Base Rule Name List and PEP Predefined Base Rule Name List.  
See “[To provision a Rule Name List table](#)” (p. 7-20)
- Provision a PCC Rule  
See “[To provision a PCC Rule table](#)” (p. 7-14)

## Steps to provision a Policy Selector table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS** → **IMS Components** → **PDF Tables**.

**Result:** The **PDF Tables** window is displayed.

---

- 2 In the left pane, expand the **Policy Selector Table** folder.

**Result:** The Policy Selector tables are listed under the folder in the left pane.

If the folder is empty, add a Policy Selector table.

Perform the following steps in the **PDF Tables** window to add, rename, or delete a Policy Selector table :

| If you want to ...              | then ...  |
|---------------------------------|---|
| add a Policy Selector table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add Policy Selector Table table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a Policy Selector table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename Policy Selector Table table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete a Policy Selector table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Policy Selector table, ensure that no table entries are in use.</p> <p><i>End of steps</i></p>   |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the Policy Selector table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **PDF Tables** window to add, modify, or delete the Policy Selector table attributes:

| If you want to ...                         | then ...  |
|--|---|
| add the Policy Selector table attributes,  | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Policy Selector Table</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a Policy Selector table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Policy Selector Table</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a Policy Selector table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                     |

5 **Note:**

- Subscriber Tier ID is the key to Session Initial Policy Selectors.
- Subscriber Tier ID and QoS Class Identifier are key to AF Modification Policy Selectors and Non-AF Modification Policy Selectors.
- For each entry, at least one of the three Rule (Lists) must be selected and for each type, at least one entry must be provisioned.
- The maximum count for Session Initial Policy Selector is 20, and for AF Modification Policy Selector and Non-AF Modification Policy Selector is 60.

Provision the following parameters:

| Parameter                                 | Provisioning   |
|---|--|
| <b>Policy Selector Type</b>               | Select the Policy Selector type.<br>The following are the available options: <ul style="list-style-type: none"> <li>• AF Modification</li> <li>• Non AF Modification</li> <li>• Session Initialization</li> </ul> <b>Note:</b> When Session Initialization is selected, the IP-CAN Session parameter is unavailable. |
| <b>Subscriber Tier ID</b>                 | Select a Subscriber Tier to associate with the Policy Selector Table.  |
| <b>QoS Class Identifier</b>               | Select the Qos Class Identifier.<br>This parameter is available for <b>AF Modification</b> and <b>Non-AF Modification</b> Policy Selector  |
| <b>PEP Predefined Rule Name List</b>      | Select the PEP Predefined Rule Name List.  |
| <b>PEP Predefined Base Rule Name List</b> | Select the PEP Predefined Base Rule Name List  |
| <b>PCC Rule</b>                           | Select the PCC Rule.<br>This parameter is available for <b>AF Modification</b> type only.  |
| <b>PCC Rule List</b>                      | Select the PCC Rule List<br>This parameter is available for <b>Non AF Modification</b> and <b>Session Initialization</b> types.  |

For more information on the parameters, see the topic **Policy Selector Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

6 Click **OK**.

**Result:** The Policy Selector table attributes are provisioned successfully.

END OF STEPS

# TISPAN RACS

## Overview

### Purpose

This section provides the task flow to configure TISPAN RACS and procedures that are specific to TISPAN RACS configuration.

### Contents

|                                      |      |
|--------------------------------------|------|
| To add an H.248 Device Server        | 7-29 |
| To provision an H.248-controlled BGW | 7-32 |
| To provision a DSCP Profile table    | 7-36 |

# To add an H.248 Device Server

## Purpose

This procedure provides the steps to provision an H.248 device server (DS) as a component in an existing component group.

## Description

An H.248 device server is a logical component that is co-resident with the NGSS service on the same card in the ATCA platform. An H.248 device server processes H.248 protocol messages that are used to control various types of media gateways.

The H.248 service resides on the same physical host as the IMS server service. This increases the capacity of the configuration by more efficiently using the hosts that currently exist in the chassis.

**Note:** Provision the H.248 service on the same card/host/blade slot number as the desired IMS server service.

## Before you begin

When you want to add a H.248 Device Server, ensure that you have checked the following:

- The H.248 Service must be added through service growth or field installation prior to provisioning the H.248 service on the card.

See chapter *Manage System Configuration - Hardware Growth* in the guide, *Alcatel-Lucent 5400 Linux Control Platform Configuration Management*, 270-702-014 for more information.

## Steps to provision an H.248 Device Server

Perform the following steps at the Provisioning GUI:

- 
- 1 Click **System View**.

**Result:** The **System View** window is displayed.

---

- 2 In the left pane, expand the component group name.

| 3 | If you want to     | Then   |
|---|--------------------|--|
|   | Add an H.248 DS    | <p>Do the following:</p> <ol style="list-style-type: none"> <li>From the <b>Components</b> menu, choose <b>Add Service</b>.</li> <li>Proceed with <a href="#">Step 4</a>.</li> </ol>   |
|   | Modify an H.248 DS | <p>Do the following:</p> <ol style="list-style-type: none"> <li>Select the DS that you want to modify</li> <li>From the <b>Components</b> menu, choose <b>Modify</b>.</li> <li>In the <b>Alcatel-Lucent Control Platform - System Service Configuration</b> window that appears, change the parameters, and then click <b>Finish</b>.</li> <li>Proceed with <a href="#">Step 7</a>.</li> </ol> |
|   | Delete an H.248 DS | <p>Do the following:</p> <ol style="list-style-type: none"> <li>Select the DS that you want to delete.</li> <li>From the <b>Components</b> menu, choose <b>Delete</b>.</li> <li>In the dialog box that appears, click <b>Yes</b> to confirm.</li> <li>Proceed with <a href="#">Step 7</a>.</li> </ol>  |

- 4 In the first screen of the **Alcatel-Lucent Control Platform - System Component Configuration** window that appears, provision as follows:

| Parameter               | Provisioning   |
|-------------------------|--|
| <b>Component Name</b>   | Type a descriptive name  |
| <b>Component Family</b> | Select <b>Device Server</b>  |
| <b>Component Type</b>   | Select <b>H.248 DS</b>   |
| <b>Pair Information</b> | Select the pair of redundant cards of your choice.<br>The control IP addresses are automatically assigned accordingly. |

Click **Next**.

- 
- 5 In the second screen of the **Alcatel-Lucent Control Platform - System Component Configuration** window, provision as follows:

| Parameter             | Recommended provisioning |
|-----------------------|--------------------------|
| Switchover Count      | 8                        |
| Poll Frequency (secs) | 001                      |
| Reconnect After       | 001                      |
| Retry Count           | 03                       |

Click **Next**.

---

- 6 In the third screen of the **Alcatel-Lucent Control Platform - System Component Configuration** window, provision as follows:

| Parameter               | Recommended provisioning   |
|-------------------------|--|
| ACR Charging Profile Id | The ACR charging Profile id defined in ISC_ACR_CHA RGING_PROFILE.  |
| Enable Binary Encoding  | No   |
| Binary Encoding Port    | 2945   |
| Enable Text Encoding    | Yes  |
| Text Encoding Port      | 2944   |
| Parameter Variant       | Select the required variant<br>To view the parameters in the selected variant, click <b>Display</b> . After the parameters are verified in the Advanced Parameters Display, click <b>Close</b> . |

Click **Finish**.

**Result:** An H.248 device server is added to the component group.

The **Alcatel-Lucent Control Platform - System Component Configuration** window is closed.

---

- 7 In System View, click the **File** menu, and then click **Exit**.

END OF STEPS

---

# To provision an H.248-controlled BGW

## Purpose

This procedure provides the steps to provision an H.248-controlled Border Gateway (BGW).

By adding a BGW on the H.248 DS, the Diameter stack is activated on the H.248 DS, creating a Border Gateway Controller.

## Before you begin

Ensure that the IP logical control address of the BGW is available

IP connections must exist between the border gateways and the H.248 DS on the LCP.

## Steps to provision an H.248-controlled BGW

Perform the following steps at the Provisioning GUI:

- 1 Click **System View**.

**Result:** The **System View** window is displayed.

- 2 In the left pane, expand the Gateways folder.

**Result:** The Gateways are listed under the folder in the left pane.

Perform the following steps in the **System View** window to add, modify, or delete an H.248-controlled BGW :

| If you want to ...             | then ...  |
|--------------------------------|---|
| add a H.248-controlled BGW,    | <ol style="list-style-type: none"> <li>1. Select <b>Components</b> → <b>Add a Gateway</b>.<br/><b>Result:</b> The <b>Linux Control Platform - System Component Configuration</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a></li> </ol>       |
| modify a H.248-controlled BGW, | <ol style="list-style-type: none"> <li>1. Select the gateway, and then select <b>Components</b> → <b>Modify</b>.<br/><b>Result:</b> The &lt;window name&gt; window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a></li> </ol> <p><i>End of steps</i></p> |

| If you want to ...             | then ...  |
|--------------------------------|---|
| delete a H.248-controlled BGW, | <ol style="list-style-type: none"> <li>Select the gateway, and then select <b>Components → Delete</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p> |

- 3 Provision the following parameters in the first part of the **Linux Control Platform - System Component Configuration** window :

| Parameter                    | Recommended value  |
|------------------------------|--|
| <b>Component Name</b>        | A descriptive name (any ASCII string).   |
| <b>Component Family</b>      | Select <b>Gateway</b>  |
| <b>Component Type</b>        | Select <b>Border GW</b>  |
| <b>Component Number</b>      | Select the default number  |
| <b>GW IP Connection Type</b> | The BGC decides what type of signaling transport connection to support with the BGW based on the setting of this field.  |
| <b>IP Address 1</b>          | Type the logical primary IP control address for this BGW.<br><i>Important:</i> A floating IP address is preferred.<br>This field is an edit box for BGW. Otherwise, it is an IP control box. |
| <b>IP Address 2</b>          | 0.0.0.0<br>This field is an edit box for BGW. Otherwise, it is an IP control box.  |

**Notes:**

- GW IP Connection Type** can be enabled only if the **Component Type** is set to "Border GW". Only if **Component Type** is set to "Border GW" and **Connection Type** is "UDP/IP", the value for **GW IP Connection Type** can be "IPv6" or "IPv4 and IPv6".
- If **GW IP Connection Type** is set to "IPv4", then the **IP Address 1** and **IP Address 2** can be entered for both "IPv4 address", or one "IPv4 address" and the other address is empty. At least one GW IPv4 address must be provisioned, but optionally, an IPv6 address is allowed in the other address.
- If **GW IP Connection Type** is set to "IPv6", then the **IP Address 1** and **IP Address 2** can be entered both "IPv6 address", or one "IPv6 address" and the other address is empty. At least one GW IPv6 address must be provisioned, but optionally, an IPv4 address is allowed in the other address.
- If **GW IP Connection Type** is set to "IPv4 and IPv6", then the **IP Address 1** and **IP Address 2** are both shown as edit control and both allow IPv4 and IPv6 address, one of the IP Addresses can be empty, but not both.

- 4 Click **Next**.

**Result:** The second part of the **Linux Control Platform - System Component Configuration** window is displayed.

- 5 Provision the following parameters with recommended values:

| Parameter                 | Recommended value   |
|---------------------------|---|
| Protocol Selection        | Select <b>H.248</b> .   |
| GW Vendor                 | Select <b>ExternalGW</b> .  |
| Call Control Device Assoc | Designate the H.248 Device Server that controls this BGW.<br>An H.248 Device Server can control multiple Border Gateways. |

- 6 Click **Next**.

**Result:** The third part of the **Linux Control Platform - System Component Configuration** window is displayed.

- 7 In the **Local Termination Types** section, select **RTP/UDP/IP** and use the following values:

| Parameter         | Value      |
|-------------------|------------|
| RTP/UDP/IP Prefix | I/1/access |

- 8 In the **Network Termination Types** section, select **RTP/UDP/IP** and use the following values:

| Parameter         | Value       |
|-------------------|-------------|
| RTP/UDP/IP Prefix | I/1/network |

- 9 In the **MGC-MG Interface** section, use the following values:

| Parameter       | Recommended value |
|-----------------|-------------------|
| Connection Type | UDP/IP            |

10 Click **Next**.

**Result:** The fourth part of the **Linux Control Platform - System Component Configuration** window is displayed.

11 Click **Next**.

**Result:** The fifth part of the **Linux Control Platform - System Component Configuration** window is displayed.

12 For the **H.248 configuration**, use the following recommended values:

| Parameter      | Recommended value |
|----------------|-------------------|
| Context Audits | <b>None</b>       |

13 In the **Advanced Provisioning** section, use the following recommended values.

| Parameter         | Recommended value   |
|-------------------|---|
| Parameter Variant | Select the H.248 GW variant<br><i>Note:</i> Before selecting the GW variant, create the variant by clicking <b>System Admin</b> → <b>Variants</b> → <b>H248 GW Variants</b> . |

To view the values for a selected variant, click **Display**:

For more information on the parameters, see the topic **H.248 gateway** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

14 Click **Finish**.

**Result:** The Border GW shows as a logical component in the **System View - Gateways** window.

END OF STEPS

# To provision a DSCP Profile table

## Purpose

This procedure is used to add, modify, or delete a DSCP profile.

## Steps to provision a DSCP table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Components** → **PDF Tables**.

**Result:** The **PDF Tables** window is displayed.

- 2 In the left pane, expand the **DSCP Profile** folder.

**Result:** The DSCP Profile tables are listed under the folder in the left pane.

If the folder is empty, add a DSCP profile table.

Perform the following steps in the **PDF Tables - DSCP Profile** window to add, rename, or delete a DSCP Profile table :

| If you want to ...           | then ...  |
|------------------------------|---|
| add a DSCP Profile table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add DSCP Profile table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.<br/><i>End of steps</i></li> </ol> |
| rename a DSCP Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename DSCP Profile table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.<br/><i>End of steps</i></li> </ol>  |

| If you want to ...           | then ...  |
|------------------------------|---|
| delete a DSCP Profile table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a DSCP Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the DSCP Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **PDF Tables - DSCP Profile** window to add, modify, or delete the DSCP Profile table attributes:

| If you want to ...                      | then ...   |
|---|--|
| add the DSCP Profile table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify a DSCP Profile table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>DSCP Profile attributes</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                      | then ...  |
|---|---|
| delete a DSCP Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

5 Provision the following parameters:

| Parameter                          | Provisioning  |
|------------------------------------|---|
| <b>Dscp Profile Id</b>             | Select a unique ID for the DSCP profile.  |
| <b>Conversational Traffic</b>      | Select a Diffserv Codepoint value that is assigned to Conversational class traffic. |
| <b>Streaming Traffic Class</b>     | Select a Diffserv Codepoint value that is assigned to Streaming class traffic.      |
| <b>Interactive 1 Traffic Class</b> | Select a Diffserv Codepoint value that is assigned to Interactive-1 class traffic.  |
| <b>Interactive 2 Traffic Class</b> | Select a Diffserv Codepoint value that is assigned to Interactive-2 class traffic.  |
| <b>Interactive 3 Traffic Class</b> | Select a Diffserv Codepoint value that is assigned to Interactive-3 class traffic.  |
| <b>Background Class</b>            | Select a Diffserv Codepoint value that is assigned to Background class traffic.     |

For more information on the parameters, see the topic **DSCP Profile** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

6 Click **OK**.

**Result:** The DSCP Profile table attributes are provisioned successfully.

END OF STEPS





# Part IV: Accounting management

## Overview

### Purpose

This part of the documentation provides procedures to perform Accounting Management tasks.

### Contents

|   |     |
|---|-----|
| <a href="#">Chapter 8, Offline charging</a> | 8-1 |
| <a href="#">Chapter 9, Online charging</a>  | 9-1 |



# 8 Offline charging

## Overview

### Purpose

This chapter provides procedures to perform offline charging-related accounting management tasks.

### Contents

|   |             |
|---|-------------|
| <b>Provision ACR task flow</b>                                      | <b>8-2</b>  |
| To activate an ACR message generation on a SIPia port               | 8-3         |
| To provision an ACR Charging Profile                                | 8-5         |
| Assigning an ACR Charging profile to an IMS entity                  | 8-15        |
| ACR Consolidation Enhancement                                       | 8-18        |
| <b>Provision ACR buffering function</b>                             | <b>8-20</b> |
| ACR Buffering Function (ABF)  | 8-21        |
| To provision an ABF Diameter profile table                          | 8-24        |
| <b>Miscellaneous topics</b>   | <b>8-29</b> |
| Activate inclusion of CDMA access network information               | 8-30        |
| Checking compatibility with 3GPP Release 7 Diameter messages on CCF | 8-31        |

# Provision ACR task flow

## Overview

### Purpose

This section provides the procedures to provision the ACR.

### Contents

|   |      |
|---|------|
| To activate an ACR message generation on a SIPia port | 8-3  |
| To provision an ACR Charging Profile                  | 8-5  |
| Assigning an ACR Charging profile to an IMS entity    | 8-15 |
| ACR Consolidation Enhancement                         | 8-18 |

# To activate an ACR message generation on a SIPia port

## Purpose

This procedure is used to activate ACR message generation on an SIPia port. When ACR message generation is activated, the IMS component establishes a Rf connection to the Charging Collection Function.

## SIPia port types supporting ACR

The following SIPia port types support ACR message generation:

|        |        |      |
|--------|--------|------|
| P-CSCF | S-CSCF | IBCF |
| I-CSCF | E-CSCF | BGCF |

The following SIPia port types support ACR message generation:

- STAS

The following SIPia port types support ACR message generation for the FS 2500 application:

- HOAS
- MMAS

The following SIPia port types support ACR message generation:

- MGCF/(G)MSC

## Before you begin

This procedure assumes the SIPia port is already created.

For details about creating SIPia ports, refer to “[To provision a SIPia port](#)” (p. 10-40).

## Procedure

Perform the following steps:

- 
- 1 Select **System View** → **Component List**.

**Result:** The **System View** window is displayed.

---

- 2 In the left pane, expand the **Services** → **IMS** → **IMS Services** folder.

**Result:** The IMS Services tables are listed under the folder in the left pane.

- 
- 3 Double-click the table to open the list of profiles defined for the table.

---

  - 4 In the right pane, right-click the profile that you want to modify and select **Modify**.

---

  - 5 Select the **ACR Messages Generation** check box.

**Additional information:** Observe the following:

- When **ACR Messages Generation** check box is selected and **Administrative State** is *unlock*, the ACR message generation and the Rf connection are open.
- When **ACR Messages Generation** check box is unchecked or **Administrative State** is *lock*, the Rf connection is torn down and ACR generation is disabled.
- If an SIPia port is shut down, the Rf connection and ACR generation remains unchanged.

- 
- 6 Click **OK**.

---

END OF STEPS

---

# To provision an ACR Charging Profile

## Purpose

This procedure is used to provision an ACR Charging Profile.

## Before you begin

**Note:** An ACR Charging Profile with ID 0 is regarded as a default profile. The default profile is mapped to 3GPP version 5 ACR messages for an existing system (for a new installation, the default profile is mapped to 3GPP version 8 ACR messages). The content of default profile is not modified through the FS GUI. If you need to change the version, add a new ACR charging profile with the expected version selection and correlate the application to the new ACR charging profile.

## Steps to provision an ACR Charging Profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS > IMS Tables**.

**Result:** The **IMS Tables** window is displayed.

- 2 In the left pane, expand the **IMS > General > ACR Charging Profile** folders.

**Result:** The ACR Charging Profile tables are listed under the folder in the left pane.

If the folder is empty, add an ACR Charging Profile table.

Perform the following steps in the **IMS Tables** window to add, rename, or delete an ACR Charging Profile table:

| If you want to ...                 | then ...   |
|------------------------------------|--|
| add an ACR Charging Profile table, | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add ACR Charging Profile table</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |

| If you want to ...                    | then ...   |
|---------------------------------------|--|
| rename an ACR Charging Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename ACR Charging Profile table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete an ACR Charging Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an ACR Charging Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>                 |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the ACR Charging Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** Perform the following steps at the **ACR Charging Profile** window to add, modify, or delete the ACR Charging Profile table attributes:

| If you want to ...                             | then ...  |
|--|---|
| add the ACR Charging Profile table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>ACR Charging Profile</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                               | then ...   |
|--|--|
| modify an ACR Charging Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>ACR Charging Profile</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete an ACR Charging Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                        |

**5** Provision the following parameters:

| Parameter                        | Provisioning   |
|----------------------------------|--|
| <b>ACR Charging Profile ID</b>   | Enter the appropriate ACR Charging Profile Id.<br><br>The range for ACR Charging Profile ID is 0 to 256. The default value is 0.   |
| <b>Version Control Selection</b> | Select the value for the desired ACR Version Control Selection.<br><br><b>Note:</b> The ACR Charging Profile also supports V9 ACR in addition to V5 ACR, V7 ACR and V8 ACR. The option 3GPP 32.260 Rel X.Y has to be selected in the Version Control Selection list to send V9 ACR and above messages. The values for X and Y are configurable in the fields <b>Release Number</b> and <b>Extension Number</b> respectively. |

| Parameter               | Provisioning   |
|-------------------------|--|
| <b>Release Number</b>   | <p>This parameter specifies the 3GPP Release number. This field can be set only if the Version Control is set to 3GPP 32.260 Rel X.Y.</p> <p>The value ranges from 9 to 99. The default value is 9.</p> <p><b>Note:</b> When the Version is set to Rel 5.7.0 or Rel 7.4.0 or Rel 8.6.0, the field <b>Release Number</b> is grayed out and cannot be modified.</p>                                |
| <b>Extension Number</b> | <p>This parameter specifies the extension number of the provisioned 3GPP Release. This field can be set only if the Version Control is set to 3GPP 32.260 Rel X.Y.</p> <p>The value ranges from 0 to 25. The default value is 0.</p> <p><b>Note:</b> When the Version is set to Rel 5.7.0 or Rel 7.4.0 or Rel 8.6.0, the field <b>Extension Number</b> is grayed out and cannot be modified.</p> |

**Notes:**

- When the ACR Charging Profile is provisioned in the H.248 table, the fields **Version Control Selection** and **Use HSS Provided CCF Address** cannot be modified.

Under **Detailed ACR Message Generation Options** group, select values for the following attributes:

| Parameter   | Description  |
|---|--|
| <b>For P-CSCF/ S-CSCF/ I-CSCF/ IBCF/ BGCF/ E-CSCF/ AGCF</b> |  |
| <b>INVITE Dialog</b>  | <p>This parameter gives the service provider an option to turn on ACR messages generation for INVITE dialog when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b>.</p> <p><b>Note:</b> This flag does not control AGCF.</p>  |
| <b>Initial INVITE Error Cases</b>                           | <p>This parameter gives the service provider an option to turn on generating ACR (Event) messages for failure cases, when it tries to establish an INVITE dialog, when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b>.</p> |
| <b>For P-CSCF/ SCSCF/ I-CSCF/ IBCF/ BGCF</b>                |  |

| Parameter                              | Description   |
|--|---|
| <b>REFER Dialog</b>                    | This parameter gives the service provider the option to turn on ACR messages generation for REFER dialog when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> .                    |
| <b>SUBSCRIBE Dialog</b>                | This parameter gives the service provider the option to turn on ACR messages generation for SUBSCRIBE dialog when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> .                |
| <b>NOTIFY Transaction</b>              | This parameter gives the service provider the option to turn on ACR messages generation for NOTIFY transaction when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> .              |
| <b>PUBLISH Transaction</b>             | This parameter gives the service provider the option to turn on ACR messages generation for PUBLISH transaction when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> .             |
| <b>MESSAGE Transaction</b>             | This parameter gives the service provider the option to turn on ACR messages generation for MESSAGE transaction when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> .             |
| <b>REFER Error Cases</b>               | This parameter gives the service provider the option to turn on ACR messages generation for REFER Dialog Error Cases when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> .        |
| <b>SUBSCRIBE Error Cases</b>           | This parameter gives the service provider the option to turn on ACR messages generation for SUBSCRIBE Dialog Error Cases when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> .    |
| <b>NOTIFY Transaction Error Cases</b>  | This parameter gives the service provider the option to turn on ACR messages generation for NOTIFY Transaction Error Cases when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> .  |
| <b>PUBLISH Transaction Error Cases</b> | This parameter gives the service provider the option to turn on ACR messages generation for PUBLISH Transaction Error Cases when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> . |
| <b>MESSAGE Transaction Error Cases</b> | This parameter gives the service provider the option to turn on ACR messages generation for MESSAGE Transaction Error Cases when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> . |
| <b>For P-CSCF/S-CSCF/ I-CSCF/ IBCF</b> |   |
| <b>REGISTER Transaction</b>            | This parameter gives the service provider the option to turn on ACR messages generation for REGISTER transaction when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> .            |

| Parameter                                   | Description   |
|---|---|
| <b>REGISTER Transaction for Error Cases</b> | This parameter gives the service provider the option to turn on generating ACR (Event) messages for error response to REGISTER transaction.   |
| <b>SUBSCRIBE Dialog for Reg Event</b>       | This parameter gives the service provider the option to turn on generating ACR messages for SUBSCRIBE Transaction for Reg Event when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> .   |
| <b>For P-CSCF/ S-CSCF / IBCF</b>            |   |
| <b>REINVITE without SDP Cases</b>           | This parameter gives the service provider the option to turn on generating ACR (Interim) messages for REINVITE without SDP when it tries to establish a REINVITE dialog and when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> . |
| <b>UPDATE without SDP Cases</b>             | This parameter gives the service provider the option to turn on generating ACR (Interim) messages for UPDATE without SDP when it tries to establish an UPDATE dialog and when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> .    |
| <b>NOTIFY Transaction for Reg Event</b>     | This parameter gives the service provider the option to turn on generating ACR messages for NOTIFY Transaction for Reg Event when the <b>ACR Messages Generation</b> option in the SIPia Port is set to <b>Yes</b> .  |
| <b>For P-CSCF / S-CSCF</b>                  |   |

| Parameter                     | Description  |
|-------------------------------|--|
| <b>UE Originated Requests</b> | <p>This parameter gives the service provider the option to turn on ACR messages generation for UE Originated requests, when one or more ACR Message Generation Options among:</p> <ul style="list-style-type: none"> <li>• INVITE Error Case</li> <li>• REFER Dialog</li> <li>• REFER Error Cases</li> <li>• NOTIFY Transaction</li> <li>• NOTIFY Transaction Error Cases</li> <li>• SUBSCRIBE Dialog</li> <li>• SUBSCRIBE Error Cases</li> <li>• PUBLISH Transaction</li> <li>• PUBLISH Transaction Error Cases</li> <li>• MESSAGE Transaction</li> <li>• MESSAGE Transaction Error Cases</li> <li>• MESSAGE Transaction Error Cases</li> <li>• SUBSCRIBE Dialog for Reg Event</li> <li>• NOTIFY Transaction for Reg Event</li> </ul> <p>are turned on and the <b>ACR Messages Generation</b> option in SIPia Port is set to <b>Yes</b>.</p>  |
| <b>UE Terminated Requests</b> | <p>This parameter gives the service provider the option to turn on ACR messages generation for UE Terminated requests, when one or more ACR Message Generation Options among :</p> <ul style="list-style-type: none"> <li>• INVITE Error Case</li> <li>• REFER Dialog</li> <li>• REFER Error Cases</li> <li>• NOTIFY Transaction</li> <li>• NOTIFY Transaction Error Cases</li> <li>• SUBSCRIBE Dialog</li> <li>• SUBSCRIBE Error Cases</li> <li>• PUBLISH Transaction</li> <li>• PUBLISH Transaction Error Cases</li> <li>• MESSAGE Transaction</li> <li>• MESSAGE Transaction Error Cases</li> <li>• MESSAGE Transaction Error Cases</li> <li>• SUBSCRIBE Dialog for Reg Event</li> <li>• NOTIFY Transaction for Reg Event</li> </ul> <p>are turned on and the <b>ACR Messages Generation</b> option in SIPia Port is set to <b>Yes</b>.</p> |

| Parameter                                | Description  |
|--|--|
| <b>For P-CSCF</b>                        |  |
| <b>INVITE Dialog for Emergency Calls</b> | This parameter gives the service provider the option to turn on generating ACR (Start/Interim/Event/Stop) for emergency calls only. This option can be set to <b>Yes</b> only if options INVITE Dialog, Initial INVITE Error Cases and UE Originated Requests are set to <b>No</b> . |

Provision values for the following attributes in the **Detailed ACR Message AVP Population Options** group.

| Parameter  | Description  |
|--|--|
| <b>General</b>                                   |  |
| <b>Offline Charging Time Stamp Fraction</b>      | This parameter gives the service provider the option to let the IMS NEs include SIP Request Time Stamp Fraction, SIP Response Time Stamp Fraction and SIP-Ringing-Timestamp-Fraction AVPs in the ACR messages.   |
| <b>For P-CSCF / IBCF</b>                         |  |
| <b>Proprietary AVP for VG Session BW Control</b> | Select the <b>Proprietary AVP for VG Session BW Control</b> check box to include the proprietary AVP for the virtual group session and bandwidth control, in the ACR.  |
| <b>For P-CSCF</b>                                |  |
| <b>Special AVP for Access Network Identifier</b> | This parameter gives the service provider the option to let the P-CSCF include the proprietary AVP, Access-Network- Charging-Physical-Access-ID in the ACR messages.   |
| <b>SIP Ringing Timestamp</b>                     | This parameter holds the time in UTC format of the SIP Ringing Message (180 Ringing). This is the timestamp of the first SIP 180 or 183 that contains the SDP if no 180 is received and if the FS GUI option is set to yes. It applies to P-CSCF / S-CSCF. |

| Parameter                               | Description  |
|---|--|
| <b>SDP in SIP INVITE Dialog</b>         | <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• Yes</li> <li>• Media Line Only</li> <li>• No</li> </ul> <p><b>Note:</b> This parameter gives the service provider the option to include SDP information with or without SDP-Media-Description (option set to “Yes” or “Media Line Only” ) or not to include SDP (option set to “No” ) in the ACR messages.</p>                                    |
| <b>Use HSS Provided CCF Address</b>     | <p>Select the check box if the CCF address is provided by the HSS.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• If this feature is locked, the status of the check box cannot be changed.</li> <li>• Before locking this feature, clear the check box.</li> <li>• During start-up, if this check box is selected and the feature is locked, the host automatically clears the check box.</li> </ul>                |
| <b>CT Private AVPs</b>                  | <p>Select the check box, if the CT Private AVP should be sent in the ACR.</p> <p><b>Note:</b> This field will be disabled if the Version Control Selection field is set to 32.225 Rel 5.7.0.</p>   |
| <b>Support Custom ACR Consolidation</b> | <p>Select the check box to support (turn on) custom ACR consolidation. If this check box is selected, then the S-CSCF only sends one consolidated ACR to CCF for a session that has same ICID. Only one called party answers the call, such as basic call, call forwarding, and sequential ringing services.</p> <p>In other words, this check box is used to decide if the ACR messages on S-CSCF need to be consolidated or not.</p> |

| Parameter  | Description  |
|--|--|
| <b>Custom Specific Handling for Call Diversion</b> | <p>Select the check box to support (turn on) CT specific handling for call diversion. If this check box is selected, then the Role-of-Node is set to 4(call forwarding) for call forwarding leg of the call in the ACR. The S-CSCF only generates one call forwarding ACR (that means the terminating ACR will be suppressed).</p> <p>In other words, this check box is used to decide if the S-CSCF serving forwarding subscriber needs to generate a call-forwarding ACR message(Role-Of-Node is set 4) and then suppress the terminated ACR message for B party. When the CT Specific Handling for Call Diversion check box is selected, the terminating ACR for B party is suppressed only when the S-CSCF receives a "181 Call Is Being Forwarded" message with B party number that is located in the last two indexes.</p> |
| <b>Allow ABF</b>                                   | <p>This parameter indicates if an IMS NE, which uses this ACR profile, is allowed to send undelivered ACRs to ABF when CCF is unreachable on this NE.</p> <p><b>Note:</b> This flag can be enabled only if the software licence key "IABF" is unlocked.</p>  |

For more information on the parameters, see the topic, **IMS ACR Charging Profile** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

END OF STEPS

# Assigning an ACR Charging profile to an IMS entity

## Overview

This procedure provides the steps to assign an ACR Charging profile to an IMS entity.

Assigning an ACR charging profile provides additional control about when ACR messages are generated. Using the additional control options is optional.

**Note:** ACR Charging Profile with ID 0 is regarded as a default profile. The default profile is mapped to 3GPP version 5 ACR messages for an existing system. (For a new installation, the default profile is mapped to 3GPP version 7 ACR messages). The content of default profile is not changeable through the FS GUI. If the S-CSCF is correlated to default profile and you need to change the version, you can add a new ACR charging profile with the expected version selection and associate the S-CSCF to the new ACR charging profile.

## IMS entities supporting ACR

The following IMS entities support additional ACR control by assigning an ACR Charging Profile to the profile of the IMS entity.

- P-CSCF
- S-CSCF
- I-CSCF
- E-CSCF
- BGCF
- IBCF

## Before you begin

Observe the following:

Ensure that an ACR Charging profile is configured.

## System requirements

Feature server GUI connection.

## Procedure

Perform the following steps:

- 1 At the FS GUI main menu:

| If you want to enable additional ACR control for ... | then ...   |
|--|--|
| P-CSCF,  | <ol style="list-style-type: none"> <li>1. Select <b>IMS → P-CSCF Tables</b></li> <li>2. Expand the + in front of the <b>P-CSCF Profile</b>.</li> </ol>             |
| S-CSCF,  | <ol style="list-style-type: none"> <li>1. Select <b>IMS → IMS Tables → IMS → S-CSCF</b></li> <li>2. Expand the + in front of the <b>S-CSCF Profile</b>.</li> </ol> |
| E-CSCF,  | <ol style="list-style-type: none"> <li>1. Select <b>IMS → IMS Tables → IMS → E-CSCF</b></li> <li>2. Expand the + in front of the <b>E-CSCF Profile</b>.</li> </ol> |
| I-CSCF,  | <ol style="list-style-type: none"> <li>1. Select <b>IMS → IMS Tables → IMS → I-CSCF</b></li> <li>2. Expand the + in front of the <b>I-CSCF Profile</b>.</li> </ol> |
| BGCF,  | <ol style="list-style-type: none"> <li>1. Select <b>IMS → IMS Table → IMS → BGCF</b></li> <li>2. Expand the + in front of the <b>BGCF Profile</b>.</li> </ol>      |
| IBCF,  | <ol style="list-style-type: none"> <li>1. Select <b>IMS → IMS Table → IMS → IBCF</b></li> <li>2. Expand the + in front of the <b>IBCF Profile</b>.</li> </ol>      |

- 2 Right-click the desired profile table and select **Open** from the menu.
- 3 In the right pane, select a profile, right-click a value from the table, and select **Modify Table Attributes**.
- 4 Select a profile ID in the **ACR Charging Profile ID** parameter to enable ACR for the IMS entity.

**Additional information:** When no profile is assigned (0 -> Default Options), the default options for a profile are used.

**Note:** Support for 3GPP Rel 7 :

Following is the list of ACR Charging profile IDs for 3GPP Rel 7:

- ACR Charging Profile ID for S-CSCF is '3'
- ACR Charging Profile ID for P-CSCF is '1'
- ACR Charging Profile ID for I-CSCF is '0'
- ACR Charging Profile ID for BGCF is '0'
- ACR Charging Profile ID for E-CSCF is '0'
- ACR Charging Profile ID for IBCF is '0'

5 Click **OK**.

**Result:** Additional ACR control is used for the IMS entity.

END OF STEPS

# ACR Consolidation Enhancement

## Overview

The feature “ACR Consolidation Enhancement” describes the S-CSCF enhancements to support ACR consolidation.

With this feature, the S-CSCF consolidates multiple ACRs from the various dialogs of the session into one consolidated ACR and only sends this consolidated ACR to the CCF.

## Description

This feature provides the following functionalities:

- The ACR of the first dialog generated from the S-CSCF is used as a consolidated ACR. The additional info that are available in other ACRs of the session but not available in the consolidated ACR is added to the consolidated ACR. This only applies to the Application-Server-Information, CT-Application-Servers-State and CT-Application-Servers-Abnormal AVPs. The S-CSCF populates a complete list of contacted AS in Application-Server-Information AVP, and a complete list of abnormal AS in CT-Application-Servers-State and CT-Application-Servers-Abnormal AVPs for a session (with same ICID) in the consolidated ACR, and only sends this consolidated ACR to the CCF. Choosing the first ACR as the consolidated ACR applies to a basic call and all the call diversion services (except for call forwarding) when ODI is reused with the same ICID.
- For call forwarding, the S-CSCF sets the Role-Of-Node AVP to 4 in the call forwarding ACR if the AS initiated INVITE for the call forwarding leg contains the Orig parameter in Route header, History-Info/Diversion and P-Served-User headers. If ODI is reused (Orig is not present in the INVITE) for the call forwarding dialog, then the Role-Of-Node is still set to Origination. If both ODI and Orig are included in the INVITE, then the Orig is used to process the session including set the Role-Of-Node to 4 and ODI is ignored. The call forwarding ACR message includes all application server information contacted except for the application server that triggers the call forwarding and it is not involved into the call later again, and also in the abnormal AS list.
- In the case of call forwarding, when a backward 181 is received from the AS at the S-CSCF of the called party, and if the 181 message contains the History-Info header, and the called party number is same as the number that forwards the call by checking the content of index field in the History-info header, then the S-CSCF suppresses the terminating ACR. Note that the terminating S-CSCF only checks the History-Info header in the first received 181 message and ignores all the subsequent 181 message if received.

- For call diversion services (this excludes call forwarding), for example A calls B, then redirect to C and C answers, the S-CSCF that serves the B party only generates one terminating ACR for the initial called party B with additional C party info included in the ACR. That means, the ACR for A calls B with C party address populated in the Called-Asserted- Identity AVP. The S-CSCF that serves the A party generates one originating ACR with C party address populated in the Called-Asserted-Identity AVP, if a P-Asserted-Identity header is received in the 200 OK (INVITE) message. It is assumed that AS supports reuse of ODI and the ICID for the call is the same for all the dialogs of the call. Otherwise, multiple ACRs are still generated.
- For other services, other applications, such as
  - Click to dial
  - Auto Callback
  - Auto Recall
  - Call Completion to Busy Subscriber

If the ODI is reused, the S-CSCF also only sends a consolidated ACR, that is generated for the first dialog, to the CCF. Since the S-CSCF has no service logic info about the call, the first ACR may not be the one generated when the called party actually answers the call. For example, for Auto Recall service, it may be the ACR generated when the first 200 OK is received for announcement setup. Thus the content of the consolidated ACR, such as SIP time stamps may not be accurate. If ODI is not used, the S-CSCF still follows existing implementation and sends multiple ACRs for those services. It is also assumed that AS support reuse of ODI and the ICID for the call is the same for all the dialogs of the call. Otherwise, multiple ACRs are still generated. For origination the S-CSCF populates, in the ACR generated for the first dialog, the Requested-Party-Address AVP with the Request-URI received in the original incoming request and populate the Called-Party-Address AVP with the Request-URI sent in the outgoing request which is proxied to BGCF or I-CSCF. The P-Asserted-Identity header passed back by AS in a Re-INVITE or 200 OK (INVITE) message is used to populate the Called-Asserted-Identity AVP in the ACR of the first dialog if the content of this AVP in the ACR is "Anonymous" or blank.

The parameters **Support Custom ACR Consolidation** and **CT Specific handling for Call Diversion** have to be provisioned on the ACR Charging Profile to support ACR message generation consolidation.

See "[To provision an ACR Charging Profile](#)" (p. 8-5) for more information on these parameters.

# Provision ACR buffering function

## Overview

### Purpose

This section provides the procedures that are used to provision the ACR Buffering Function (ABF).

### Contents

|  |      |
|--|------|
| <a href="#">ACR Buffering Function (ABF)</a>               | 8-21 |
| <a href="#">To provision an ABF Diameter profile table</a> | 8-24 |

# ACR Buffering Function (ABF)

## Purpose

This topic describes the ACR Buffering Function (ABF).

## Introduction to the ABF interface

The ABF interface is an interface between the ABF client (which coexists with the Rf client) and the ABF server. This is where the temporary buffered ACRs present in the limited global temporary buffer on NGSS card, are transferred to the ABF server with large disk space storage.

ABF server creates disk files that can be retrieved by the CCF later. Like the Rf interface, the ABF interface is also based on the Diameter protocol. The ABF interface cannot be provisioned unless the Rf interface is provisioned first. The ABF interface has its own configuration data, which distinguishes it from the Rf interface. When the ABF Interface connection exists, and the RF temporary buffer is 90% full, the undelivered ACRs will be downloaded to the ACR Buffering Function (ABF) using diameter interface. The ABF server will store those ACR messages received from the ABF client to the disk files.

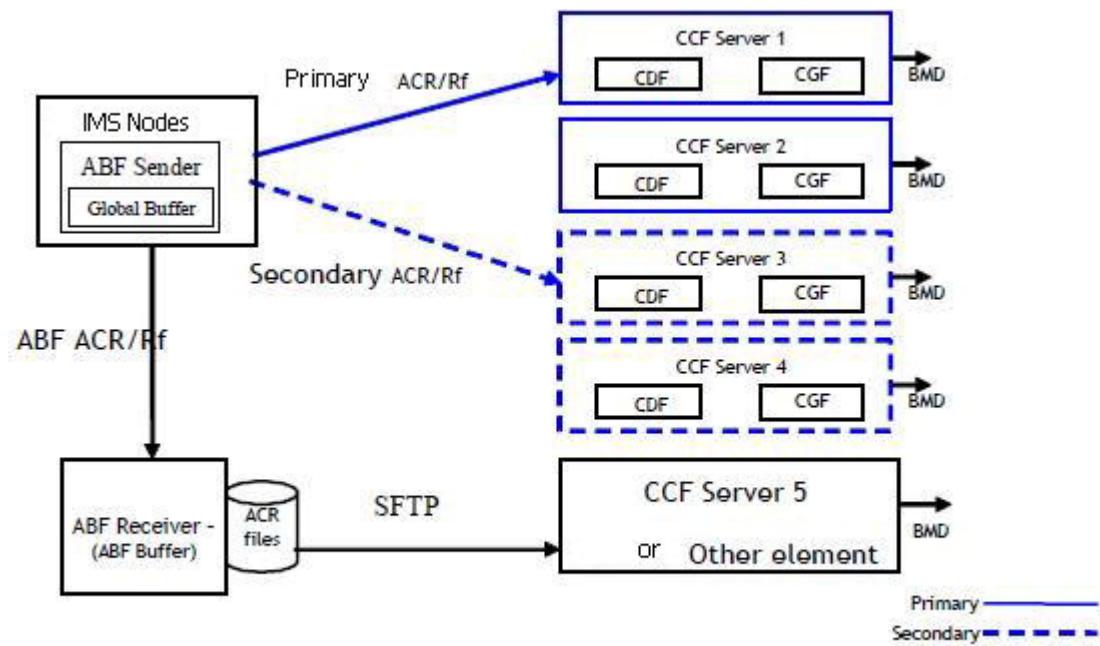
## Features supporting the ABF

The following features support the ACR Buffering Function (ABF):

- **Diameter stack and middleware:** When the Global Buffer is 90% full, the 5450 ISC (any IMS NE) will send the stored ACRs from the Global Buffer to the ABF buffer using the diameter Rf interface. Although the Rf diameter protocol is used, this interface is called proprietary ABF interface with its own provisioning view for the FQDN/IP address and other needed information for the connection.
- **ACR message buffering function:** The ACR messages will be stored in a file based on provisioned parameters, at the ABF buffer. The disk files can be retrieved by a CDF (or any other element used by the service provider) using the SFTP PULL protocol. It is expected that a new CCF server or network element other than the current primary and secondary CCF servers should be used to retrieve the ACR files, to avoid overloading a CDF that does not expect to receive offline ACR files. Each MicroCP ICS blade supports a 278 gigabyte useable RTM hard disk. For the minimal system, 175 gigabytes of the total 278 gigabytes is reserved for CTS ACR storage. Each MicroCP Distributed non-CSD CTS blade and MicroCP Distributed CSD CTS blade supports a 278 gigabyte useable RTM hard disk. For the minimal system, 123 gigabytes of the total 278 gigabytes is reserved for CTS ACR storage.

## ACR Buffering Function Network Diagram

The network diagram for the ABF mechanism is shown in the figure below:



Each 5450 ISC node is provisioned with two connections, Primary and Secondary. The ABF Buffering feature adds a third connection for backing up the ACRs. If the primary connection is down, the secondary will be used to deliver the ACR messages. If both primary and secondary connections are unable to handle the traffic and the global temporary buffer is full, the ACR messages will be sent to the backup connection. Certain criteria are verified to determine whether ACR messages should be sent to the ABF Rf connection. The relationship between the ISC and ABF is configurable. The ABF Buffer does not have to know whether it acts as a primary, secondary or ABF server. It only has to know whether the 3GPP CDR or ACR files should be created.

### Handling of ACRs

If both primary and secondary connections are down, the ACRs will be sent to the Global Buffer. When the Global Buffer is full, the ACR messages will be sent to the optional ABF Buffer solution for storage, if provisioned. If there is no ABF buffer (that is, when ABF is not provisioned), then Global Buffer will be 100 % full. As this Global Buffer is circular global temporary buffer, the older ACR messages will be overwritten. Thus the older ACR messages will be discarded and newer ACR messages will be saved.

To summarize, if both primary and secondary connections are unable to handle the traffic and the Global Buffer is full, the ACR messages will be sent to the backup connection.

The Global temporary buffer temporarily stores undeliverable ACR messages in the following cases:

- When 3004 result code is received in an ACA message
- No CCF link case - If the link to that CCF goes down, and if the link is not up within 15 minutes, then those waiting ACRs will be moved to the Global Buffer.
- No ACA Response from CCF
- For 4002 and 4003 result code case

The CCF link will apply a shedding factor in the cases below:

- When 3004/4002/ 4003 result code is received in an ACA message
- No ACA Response from CCF

The buffered ACR messages in the global temporary buffer will be resent or sent to an alternate CCF later if the alternative CCF is connected without a shedding factor. The temporary buffer size can hold ACR messages for up to 40,000 Rf sessions for each service instance.

If the Global Buffer is more than 90% full, then all the ACR messages will be sent to the provisioned ABF buffer. If there is no ABF buffer (when ABF is not provisioned), then Global Buffer will be 100 % full. As this Global Buffer is a circular global temporary buffer , the older ACR messages will be overwritten. Thus the older ACR messages will be discarded and the newer ACR messages will be saved.

For an ACA with any other error result code, the ACR message will be discarded.

# To provision an ABF Diameter profile table

## Purpose

This procedure is used to provision the Diameter profile to support ABF.

## Description

The parameters that are specified in this profile are used by the Diameter protocol stack when the messages are sent over one of the application interfaces (for example, Rf, Cx, Sh,Rx or ABF).

If there is an IMS or Converged Telephony Server (CTS) to Diameter profile mapping and the Diameter profile contains either Cx or Rf connection interfaces, then the IMS or CTS establishes a direct Diameter Cx/Rf connection to HSS/CCF.

### Diameter connection interface

The Diameter profile includes Diameter connection interfaces. The Diameter connection interfaces define which interfaces are supported in the Diameter profile. For each interface connection, the type of Diameter application and the destination or destinations are configured.

**Note:** In Diameter connection interface, provisioning the **Geographic Redundancy** and selection of **Multiple Destination Profile IDs** are mutually exclusive. That is, once the Geographic Redundancy configuration is provisioned then Multiple Destination Profile IDs will be disabled and vice versa.

## Before you begin

Before you create a Diameter port on an IMS service (for example when you are adding a PD-FE), a Diameter profile *must* be assigned to that IMS service through a service-to-Diameter mapping.

## Steps to provision a Diameter profile table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS → IMS Tables**.

**Result:** The **IMS Tables** window is displayed.

- 
- 2 In the left pane, expand the **IMS → General → Diameter Profile** folder.

**Result:** The Diameter Profile tables are listed under the folder in the left pane.

If the folder is empty, add a Diameter profile table.

Perform the following steps in the **IMS Tables** window to add, rename, or delete a Diameter profile table :

| If you want to ...               | then ...   |
|----------------------------------|--|
| add a Diameter profile table,    | <ol style="list-style-type: none"> <li>Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add Diameter Profile table</b> window is displayed.</li> <li>From the <b>Table Number</b> list, select the table number.</li> <li>In the <b>Table Name</b> box, type a descriptive table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |
| rename a Diameter profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename Diameter Profile table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |
| delete a Diameter profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Diameter profile table:</p> <ul style="list-style-type: none"> <li>Ensure that no table entries are in use.</li> <li>Ensure that none of the application interfaces (for example Rf, Cx, Sh, Rx or ABF) is operational.</li> </ul> <p><i>End of steps</i></p> |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the Diameter profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **IMS Tables** window to add, modify, or delete the Diameter profile table attributes:

| If you want to ...                       | then ...  |
|--|---|
| add a Diameter profile table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Diameter Profile</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                          | then ...  |
|---|---|
| modify a Diameter profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Diameter Profile</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol> |
| delete a Diameter profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.<br/><i>End of steps.</i></li> </ol>                |

**5** Provision the following parameters:

| Parameter                    | Provisioning   |
|------------------------------|--|
| <b>Profile ID</b>            | Type a unique ID for the Diameter profile.               |
| <b>Profile Name</b>          | Type a descriptive name for the Diameter profile.        |
| <b>Diameter Product Name</b> | Type a unique descriptive name for the diameter profile. |

The table provides information on recommended parameter values

| Parameter                         | Recommended values |
|-----------------------------------|--------------------|
| <b>DWR Message Timer</b>          | 2 sec              |
| <b>DWR Retransmission Maximum</b> | 3                  |
| <b>DWR Frequency Timer</b>        | 10 sec             |
| <b>CER Message Timer</b>          | 5 sec              |
| <b>CER Retransmission Maximum</b> | 3                  |

| Parameter               | Provisioning   |
|-------------------------|--|
| <b>Application Type</b> | Select the option ABF<br><br><b>Note:</b> The Diameter Connection Interface is for the Diameter services where the IMS service acts as a client. Only in 3GPP2, the PD-FE act as Sp' client. |

| Parameter                                       | Provisioning   |
|---|--|
| <b>Destination FQDN</b>                         | Enter the IP address of the application server in the field.<br><br>This is a Geographic Redundancy parameter.<br><br><b>Note:</b> Either a FQDN host name or an explicit IP address is allowed in this field.         |
| <b>Destination Port#</b>                        | Enter the destination port number in the field.  |
| <b>Min Percentage of Active Connections (%)</b> | Enter the minimum percentage of active connections.  |
| <b>Automatic DNS Query</b>                      | If the check box is checked, then the Diameter stack automatically queries the DNS to get the server/service IPs after a specified time. The interval is based on the DNS query status and diameter connection status. |

**Notes:**

1. For ABF application type, only primary **Destination FQDN** and primary **Destination Port#** can be provisioned. **Alternate Destination FQDN** and **Alternate Destination Port#** are not allowed to be provisioned on FSGUI.
2. To ensure DNS server is updated, click DNS Look Up. For more information, see “[Refresh DNS entry](#)” (p. 8-28)
3. For ABF application type, **Diameter Multiple Destinations Profile ID** field cannot be provisioned on FSGUI.
4. The port number entered in the **Destination Port** and (optionally) **Alt Destination Port** are for TCP connection.
5. While adding the ABF interface, Rf interface must have already existed in the same Diameter profile.
6. While deleting the Rf interface, ABF interface must be deleted first if it exists in the same Diameter profile.
7. In case of Geographic Redundancy, the “Minimum Percentage of Active Connections (%)” is a percentage of total number of connections returned when DNS query is done for Primary Server FQDN and is used to calculate the number of minimum needed connections. For Multiple Destination, the value of the “Minimum Percentage of Active Connections (%)” applies to all the FQDNs in the list. That is, the calculation of the minimum number of active DIAMETER connections is done separately for each FQDN based on the number of IP addresses returned from the DNS query. Therefore, for each FQDN the minimum number of active DIAMETER connections = ( number of query result for each FQDN ) \* ( provisioned percentage number). In both the cases, if the resulted number is a fraction, then it will be rounded up to the nearest integer number. The value ranges from 1% to 100% in increments of 1%.

For more information on the parameters, see the topic **Diameter Profile** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 6 Click OK.

**Result:** The Diameter Connection Interface attributes are provisioned successfully.

- 7 Click OK.

**Result:** The Diameter profile table attributes are provisioned successfully.

END OF STEPS

## Refresh DNS entry

Perform the following steps:

- 1 On the **Diameter Connection Interface** window, select an interface and click **Modify**.
- 2 Click **DNS Look Up**.

**Result:** The entry in the DNS server is updated.

**Important!** Applications use the FQDN to get a list of HSS/CCF IPs by querying the DNS.

To query the DNS for a list of host IPs:

1. Open the **Diameter Profile** window.
2. In the **Diameter Connection Interface** area of the window, double-click the desired application interface.
3. On the **Diameter Connection Interface** window, select the **Automatic DNS Query** check box.

**Result:** Diameter stack automatically queries the DNS to get the server/service IPs after a specified time. The interval is based on the DNS query status and diameter connection status.

END OF STEPS

# Miscellaneous topics

## Overview

### Purpose

This section provides the procedures that are used to configure offline charging.

### Contents

|   |      |
|---|------|
| Activate inclusion of CDMA access network information               | 8-30 |
| Checking compatibility with 3GPP Release 7 Diameter messages on CCF | 8-31 |

# Activate inclusion of CDMA access network information

## Overview

This procedure is used to activate CDMA access network information in the charging records.

When activated, the P-CSCF populates the Base Station ID and realm in the *Access-Network-Charging-Physical-Access-ID* Attribute Value Pair (AVP).

## Before you begin

Observe the following:

### System requirements

Feature server GUI connection.

## Procedure

Perform the following:

- 1 At the FS GUI main menu, select **IMS → IMS Components → PCSCF Tables**.

- 2 Clicking the expand '+' button to expand the **PCSCF Profile** folder.

- 3 Right click the desired profile and select **Open** to open the table.

- 4 Right click and select **Modify Table Attributes**.

**Result:** The **PCSCF Profile Attributes** window is displayed.

- 5 Select the check box **Special AVP for Access Network Identifier** to activate this function.

- 6 Click **OK**.

E N D O F S T E P S

# Checking compatibility with 3GPP Release 7 Diameter messages on CCF

## Purpose

This tool helps to check compatibility with 3GPP Release 7 Diameter messages on CCF before switching ACR version of Rf client (5450 ISC) from 3GPP Release 5 to 3GPP Release 7. This avoids the loss of billing information. The tool sends a 3GPP Release 7 test EVENT ACR message to any connected Rf servers (CCF). The message(s) ACR/ACA exchanged between the tool and associated CCF is to help safeguard that the Release 7 Diameter messages are properly handled before switching a system to operate on 3GPP Release 7.

**Note:** Only IeCCF supports 3GPP Release 7 ACR messages that have been tested by this tool. The iCCF is not tested by this tool because it does not support 3GPP Release 7 ACR messages.

## Before you begin

- The procedures documented in this topic must only be performed during low call occurrence, such as maintenance window.
- All the operations will be performed on MI active host, so before starting, the CPU usage of MI host must be monitored and it is strongly recommended that the operations are performed during low CPU usage of MI host.
- Check if the CCF on which this procedure is executed is IeCCF. This procedure must not be executed to test the iCCF.
- The existing billing interface must not be affected, when this procedure is performed. That is, the existing connections and the billing messages transmission should not be interrupted.
- For other unclear issues, contact Alcatel-Lucent technical support.

Before running this tool, verify the check box in the table below is true for the CCF and Session Manager:

|                              | Session Manager        | CCF                          | Checkbox |
|------------------------------|------------------------|------------------------------|----------|
| <b>Product</b>               | 5450 ISC               | IeCCF                        |          |
| <b>Software</b>              | Release 17.1 and above | Release ECCFR26SU8 and above |          |
| <b>ACR version supported</b> | Release 5 and 7        | Release 5 and 7              |          |
| <b>Service supported</b>     | IMS service            | Not applicable               |          |

**Procedure**

- 
- 1 Login to the active MI host as *root*.

---

  - 2 **Note:** This command needs to be executed only if you need to know the tool usage.

Execute the following command:

**`ccf_check_acr -h`**

The following output is displayed:

`ccf_check_acr -h`

Print tool help information.

`ccf_check_acr -l`

List detailed configuration information of IMS service indexed by ACR profile ID.

`ccf_check_acr -i XX`

Test all IeCCFs according to specified ACR profile ID. The XX could be one ACR profile ID, multiple profile IDs or 'all' for all ACR profile IDs.

For example:

`ccf_check_acr -i 1` : for testing ACR profile ID 1

`ccf_check_acr -i 2,3` : for testing ACR profile ID 2 and 3

`ccf_check_acr -i all` : for testing all ACR profile IDs

`ccf_check_acr -n XX`

Test all IeCCFs according to specified node number. The XX could be one node number or multiple node numbers.

For example:

`ccf_check_acr -n 256` : for testing node 256

`ccf_check_acr -n 257,258` : for testing node 257 and 258

- 
- 3 Execute the following command to know the configuration of ACR profile in 5450 ISC. This command will list ACR profile ID number, ACR version, the node number, components in related node, and the number of CCF links related with one node.

**`ccf_check_acr -l`**

The output of the command will be stored in `/var/opt/log/acr/ccf_info_acr/ACRProfileList.out`. This file will be deleted when you execute the command `ccf_check_acr -i xx` or `ccf_check_acr -n xx`.

After executing this command, you can obtain the following information:

- The number of ACR profile IDs in the site and the current version of ACR profile ID.
- The nodes and components to which these ACR profile IDs have been assigned.
- The relationship between node and CCF.

4



## WARNING

**Check the CCF IP manually to decide if it is IeCCF. If the site has CCFs other than IeCCF, then execute `ccf_check_acr` command carefully and strictly follow instructions.**

Perform one of the following steps to generate ACR Release 7 test records.

1. Test all CCFs.

If all CCFs in this site are IeCCF, then use the command `ccf_check_acr -i all`.

**Important:** If there is at least one external CCF or iCCF other than IeCCF in the site, then you must not use this command.

2. Test CCFs by ACR profile ID.

Execute the command: `ccf_check_acr -i xx`.

**Important:** If there is at least one external CCF or iCCF except IeCCF on the site, then avoid running this command format in the following situations on site.

- a. One ACR profile ID is related with iCCF or other external CCF.
- b. One ACR profile ID is related with IeCCF and iCCF or other external CCF.

Contact Alcatel-Lucent technical support for these two situations if tests must be run.

| Option (XX)           | When to use  | Example of command              |
|-----------------------|--|---------------------------------|
| Single ACR profile ID | To change the ACR version of one ACR profile ID, use this option. For example, test ACR profile ID 6.<br><br>Notes: You can also use command <code>ccf_check_acr -n 257</code> because this ACR profile ID is only used for this node. | <code>ccf_check_acr -i 6</code> |

| Option (XX)              | When to use  | Example of command                   |
|--------------------------|--|--------------------------------------|
| Multiple ACR profile IDs | To change the ACR version for multiple ACR profile IDs, use this option used. For example, change the ACR version of ACR profile ID 2, 5 and 8 at same time. | <code>ccf_check_acr - i 2,5,8</code> |

3. Test CCFs with node number.

Execute the following command: `ccf_check_acr - n XX`

**Important:** If there is at least one external CCF other than IeCCF in the site, then you must avoid running this command format in the following situations on site.

- The tested node has one ACR profile ID which is assigned into another node 9 and this node has different IeCCF. For example, if you run command `ccf_check_acr -n 1`, then you cannot switch the version of ACR profile ID 1 from Release 5 to 7 because the IeCCF2 connected with node 2 is not tested yet.
- The tested node has two CCF links, one is connected with IeCCF and the other is connected with iCCF or other external CCF.

Contact Alcatel-Lucent technical support for these two situations if tests must be run.

| Option (XX)          | When to use   | Example of command   |
|----------------------|---|--|
| Single node number   | <p>There are two situations for this option:</p> <ul style="list-style-type: none"> <li>• One new grown node<br/>If you need to create one new node 261 you can create one new ACR profile ID with Release 5, which is just assigned components on this new node. For example, node 261.</li> <li>• Multiple ACR profile IDs in one Node<br/>If you need to change the ACR version of multiple ACR profile IDs in one node, then this option can be used. For example, node 259.</li> </ul> | <code>ccf_check_acr - n 261</code><br><code>ccf_check_acr - n 259</code> |
| Multiple node number | To test multiple nodes at one time, use this option. For example, test node 257 and 258.  | <code>ccf_check_acr - n 257,258</code>                                   |

Once the correct command line format of **ccf\_check\_acr** is selected, run the command on active MI host with *root* permissions.

From the output of the command, you can obtain the following information:

- Status of ACR/ACA communication. If the status of ACR/ACA 27 communication is SUCCESS, that means ACR has been sent to CCF and ACA has been received with no errors.

CCF IP to check billing record.

**Note:** Not all components for each node will be used as ACR host to send ACR message to CCFs. In order to save resource and reduce the time of running this tool on NGSS card, only one component is selected in each node to send ACR message. For example, if customer runs command “ccf\_check\_acr –n 259”, there will be only one component. So, only one record is created if no errors occurred on CCF side.

Select the component in which the option “ACR Messages Generation” is checked in its profile. If the option “ACR Messages Generation” of all SIPia ports is not checked, then it selects the first one. Each node may be connected to multiple CCFs. A test event ACR message must be sent to each CCF. When a node is connected to multiple CCFs. A node connected to multiple CCFs will result in the billing record number per node being equal to the number of CCF links.

**Note:** For Error Handling, refer to “[Error handling for Process Errors](#)” (p. 8-36).

- 
- 5 Verify ACR Release 7 test records on CCF. Refer to the *8615 Instant Enhanced Charging Collection Function (IeCCF) Operations, Administration and Maintenance Guide*, 270-725-058 for information on how to verify the ACR Release 7 test records on IeCCF.

**Note:** To resolve any process errors refer to “[Error handling for Process Errors](#)” (p. 8-36).

**Result:** If there are no issues on the IeCCF and all billing records are correct, then you can switch the ACR version of tested ACR profile IDs from Release 5 to Release 7.

- 
- 6 Perform the following steps in the FS GUI:

1. Select **IMS** → **IMS table** → **IMS** → **General** → **ACR Charging Profile**.
2. Select **3GPP 32.260 Rel 7.40** in the **Version Control Selection** field.
3. Click **OK**.

END OF STEPS

---

## Error handling for Process Errors

Process errors reported from MI for ccf\_check\_acr :

| Error or warning information  | Analysis  | Action   |
|---|---|--|
| ccf_check_acr: Error: must be run by 'root'   | This tool must be run by user with root permission.   | Get root permission  |
| Error: Wrong number of arguments.   | Check if you have given illegal arguments.  | Run command "ccf_check_acr -h" to check what is wrong.   |
| ccf_check_acr: Invalid argument   | It was caused by wrong parameter. Such as, "ccf_check_acr -i bc". It should be "all" or numbers but "bc"  | Give correct parameter   |
| ccf_check_acr: No external CCF that needs to be provisioned and verified.   | The specified node or ACR profile ID has no connection with CCF.  | Give correct node or ACR profile ID  |
| ccf_check_acr: Error:Another ccf_check_acr process running, exit.   | 1. This tool is only run serially Only one instance of ccf_check_acr is run at same time. 2. Sometimes, it could be caused by abnormal termination. | 1. Avoid running this in parallel<br>2. Firstly, try command "ps -u root grep ccf_check_acr" to see if it is existed. If yes, kill it. If not, then delete this file /var/opt/log/acr/ccf_check.lock |
| Memory errors :<br>1. ccf_check_acr: Error: Not enough free disk under qdc07-s01c05h0:/dev/shm, skipping the node 258 .<br>2. ccf_check_acr: Error: 13500 KB memory available on qdc07-s01c05h0, at least 15MB required; Please contact A LU support. | See error information   | For these kind of errors, contact Alcatel-Lucent technical support before taking any action.   |
| No response from ccf_info_acr   | It could have tight loop or other reason led to no response from ccf_info_acr   | 1. Try test again after several minutes.<br>2. Call ALU technical support  |

| Error or warning information  | Analysis  | Action  |
|---|---|---|
| No response from rf_client_sim  | It could have tight loop or other reason led to no response from ccf_info_check       | <ol style="list-style-type: none"> <li>Try test again after several minutes.</li> <li>Call ALU technical support</li> </ol> |
| Rf_client_sim is killed   | Usually it can't be happened in normal situation.                                     | Try test again.   |
| Other Error   | N/A   | Call ALU technical support  |
| Errors reported from rf_client_sim, such as:<br>FAILURE (Connection to the CCF timeout) | Refer to Process errors from NGSS card for detailed information, analysis and action. | N/A   |

Process errors reported from MI for ccf\_info\_acr :

| Error or warning information  | Analysis  | Action  |
|---|---|---|
| Warning: ACR Profile ID 16 does not exist   | The ACR profile ID specified isn't existed. Check ACR profile ID table on FSGUI   | Give correct ACR profile ID   |
| ccf_info_acr: Warning: The specified node 262 either does not exist, or does not have IMS services assigned, or does not have Rf interface. | As it has been reported   | Give correct node   |
| ccf_info_acr: Warning: Node 257 is connected with iCCF. Skipping...   | Current, iCCF doesn't support ACR Rel 7 message, so the tool will ignore this kind of node for current version  | Don't specify the ACR profile ID or node related with iCCF  |
| ccf_info_acr: Warning: One sipia port of Node 259 is associated with ACR version 7. Skipping...   | Once the ACR version of one SIPia port is Rel 7 in one node, then this node will be ignored because it has been sent Rel 7 ACR message before and the further test isn't needed | Don't specify the ACR profile ID if it's the ACR version is Rel 7 or node which the ACR version of ACR profile assigned one component is Rel 7. |
| ccf_info_acr: Warning: Node 258 has no P/I/S/E-CSCF, IBCF and BGCF. Skipping...   | This tool only supports the following SIPia ports: P/I/S/ECSCF, IBCF and BGCF   | When you specify node, make sure that it has these SIPia ports(P/I/S/E-CSCF, IBCF and BGCF)   |

| Error or warning information   | Analysis                | Action                                      |
|--|-------------------------|---|
| ccf_info_acr: Warning: ACR profile ID 2 isn't assigned.<br>Skipping... | As it has been reported | Do not specify this kind of ACR profile ID. |

Process errors reported from CCF :

| Error or warning information             | Analysis  | Action  |
|--|---|---|
| FAILURE: (Connection to the CCF timeout) | It could be CCF can't be reachable or the IP or port isn't correct. | ISC side: <ul style="list-style-type: none"><li>• Check if diameter profile is mapping to correct card.</li><li>• Check IP and port in diameter profile whether it Alcatel-Lucent – Proprietary Use pursuant to Company Instructions. QDI ID: 38242 Version: 0 Page 17 is correct.</li></ul> CCF side: <ul style="list-style-type: none"><li>• Check CCF /etc/host/ file</li><li>• Rcv menu table 91. and 9.2. The IMS NE hostname should be provisioned in above tables.</li></ul> |
| FAILURE: (ACA timeout from the CCF)      | ACR has been sent to CCF, but CCF doesn't response.                 | CCF side: <ul style="list-style-type: none"><li>• Check CCF status if it is in IS (in service )status</li><li>• Check if CCF is too busy , CCF server CPU busy time &gt;%60</li></ul>   |

| Error or warning information      | Analysis                      | Action   |
|-----------------------------------|-------------------------------|--|
| FAILURE: (ACA error from the CCF) | Result code in ACA isn't 2001 | <p>Fix the error according to CCF result code.</p> <ul style="list-style-type: none"> <li>• Error 3002: check Rcv menu table 13.2.2 , the destination realm field should match the value of destination realm</li> <li>• Error 5001: CCF does n't support some AVPs of ACR</li> <li>• Error 5004: ACR include some invalidate AVP values.</li> </ul> |

Internal Errors :

| Error or warning information  | Analysis | Action |
|---|----------|--------|
| <p>For following errors, contact Alcatel-Lucent support</p> <ul style="list-style-type: none"> <li>• Memory Problem</li> <li>• Config File Error</li> <li>• Invalid Command Line Argument</li> <li>• Failed to Init TransLib</li> <li>• Failed to Perform Mutex Operation</li> <li>• Timeout(Mutex or conditional variable Timeout)</li> <li>• Error in Diameter</li> </ul> | N/A      | N/A    |



# 9 Online charging

## Overview

### Purpose

This chapter provides procedures to perform online charging-related accounting management tasks.

### Contents

|   |            |
|---|------------|
| <b>Online charging procedures</b>             | <b>9-2</b> |
| To provision an Online Charging Profile table | 9-3        |
| Provision S-CSCF profile for online charging  | 9-7        |

# Online charging procedures

## Overview

### Purpose

This section contains the procedures for online charging.

### Contents

|   |     |
|---|-----|
| To provision an Online Charging Profile table | 9-3 |
| Provision S-CSCF profile for online charging  | 9-7 |

# To provision an Online Charging Profile table

## Purpose

This procedure is used to provision an Online Charging Profile table.

## Before you begin

Before you *delete* a table, ensure that the profile is not used by an S-CSCF profile.

Recommend that you do not modify or delete default Profile ID=0. Profile ID=0 defines the default online charging behavior.

## Steps to provision an Online Charging Profile table

Perform the following steps at the Provisioning GUI::

- 1 Select **IMS → Global Tables**.

**Result:** The **Global Tables** window is displayed.

- 2 In the left pane, expand the **Online Charging Profile** folder.

**Result:** The Online Charging Profile tables are listed under the folder in the left pane.

If the folder is empty, add an Online Charging Profile table.

Perform the following steps in the **Online Charging Profile** window to add, rename, or delete an Online Charging Profile table :

- 3

| If you want to ...            | then ...  |
|-------------------------------|---|
| add an Online Charging table, | <p>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add Online Charging Profile</b> window is displayed.</p> <p><i>End of steps</i></p> |

| If you want to ...               | then ...   |
|----------------------------------|--|
| rename an Online Charging table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename Online Charging Profile table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete an Online Charging table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a Online Charging table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>                             |

- 
- 4 Double-click the table to open the list of profiles defined for the table.  
Add the Online Charging table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.
- 
- 5 Perform the following steps at the **Global Tables** window to add, modify, or delete the Online Charging Profile table attributes:

| If you want to ...                               | then ...   |
|--|--|
| add an Online Charging Profile table attributes, | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Online Charging Profile Attribute</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                                  | then ...   |
|---|--|
| modify an Online Charging Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Online Charging Profile Attribute</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.<br/><i>End of steps</i></li> </ol> |
| delete an Online Charging Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.<br/><i>End of steps.</i></li> </ol>                                     |

**6** Provision the following parameters:

| Parameter                           | Provisioning  |
|-------------------------------------|---|
| <b>Profile Id</b>                   | select a unique ID for the Online Charging Profile Attribute.   |
| <b>CCR For UE Originated INVITE</b> | If enabled, it determines if a Credit Control Request (CCR) message is sent to the Online Charging System for INVITE requests that originate from a UE.     |
| <b>CCR For UE Terminated INVITE</b> | If enabled, it determines if a Credit Control Request (CCR) message is sent to the Online Charging System (OCS) for INVITE requests that terminate to a UE. |

For more information on the parameters, see the topic **Online Charging Profile** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

**7** Click **OK**.

**Result:** The Online Charging Profile table attributes are provisioned successfully.

END OF STEPS

# Provision S-CSCF profile for online charging

## Purpose

This topic describes how to configure the S-CSCF for online charging.

## Procedure

Perform the following:

- 1 At the FS GUI main menu, select **IMS → IMS Tables**.
- 2 Expand **IMS → SCSCF → S-Cscf Profile**.
- 3 Select a profile table and open the table.
- 4 Select a profile ID and modify the table attributes.
- 5 Configure the following parameters for online charging:

| Parameter                         | Description   |
|-----------------------------------|---|
| <i>IMS-GWF FQDN</i>               | Enter the fully qualified domain name of the IMS-GWF that provides the interface to the online charging system.   |
| <i>Online Charging Profile ID</i> | Select a profile.<br>The profile determines the types of sessions for which online charging is used.<br>By default, the S-CSCF uses profile ID=0.<br>Profile ID=0 defines the default online charging behavior. |

END OF STEPS



# Part V: Common procedures for ISC and SPDF

## Overview

### Purpose

This part of the documentation describes procedures that are referenced by multiple provisioning task flows.

### Contents

|   |      |
|---|------|
| <a href="#">Chapter 10, Common procedures</a> | 10-1 |
|---|------|



# 10 Common procedures

## Overview

### Purpose

This chapter contains the common procedures for the IP Session Control and Service Policy Decision Function.

### Contents

|   |              |
|---|--------------|
| <b>IP session control and service policy decision function</b>  | <b>10-3</b>  |
| To connect to the CNFG host using the Provisioning GUI          | 10-4         |
| To execute the base configuration                               | 10-6         |
| To start and verify the FSDB                                    | 10-8         |
| To provision NGSS Server parameters                             | 10-9         |
| To provision an IMS Service association                         | 10-20        |
| To provision a Diameter profile                                 | 10-23        |
| To modify Diameter application IDs                              | 10-31        |
| To provision a Service to Diameter mapping                      | 10-32        |
| <b>IP session control</b>                                       | <b>10-36</b> |
| To provision an SCTP Profile                                    | 10-37        |
| To provision a SIPia port                                       | 10-40        |
| To provision ENUM server addresses                              | 10-49        |
| To provision an incoming digit table                            | 10-50        |
| To provision the ENUM profile                                   | 10-57        |
| To provision an Originating Hosts list                          | 10-64        |
| Wildcards in digit strings                                      | 10-68        |
| To change the operational state of a host providing IMS Service | 10-72        |

|   |               |
|---|---------------|
| To change the operational or administrative state of a SIPia port | 10-80         |
| To view the operational state of a host providing IMS Service     | 10-82         |
| To view the administrative state of a SIPia port                  | 10-83         |
| Verifying operational functionality using the ims_cli command     | 10-84         |
| To provision an External Domain Routing table                     | 10-99         |
| <b>Service policy decision function</b>                           | <b>10-103</b> |
| To provision a PDF profile  | 10-104        |
| To provision a Diameter port                                      | 10-108        |
| To lock, or unlock a Diameter port                                | 10-111        |
| To provision a variant  | 10-114        |
| To provision a PPL component in a signaling variant               | 10-116        |

# IP session control and service policy decision function

## Overview

### Purpose

This section contains procedures that are common for both IP Session Control and Service Policy Decision Function (SPDF) related provisioning procedures.

Some of these procedures are stand-alone procedures while the remaining are referenced from various procedures as a part of the provisioning task flows.

### Contents

|  |       |
|--|-------|
| To connect to the CNFG host using the Provisioning GUI | 10-4  |
| To execute the base configuration                      | 10-6  |
| To start and verify the FSDB                           | 10-8  |
| To provision NGSS Server parameters                    | 10-9  |
| To provision an IMS Service association                | 10-20 |
| To provision a Diameter profile                        | 10-23 |
| To modify Diameter application IDs                     | 10-31 |
| To provision a Service to Diameter mapping             | 10-32 |

# To connect to the CNFG host using the Provisioning GUI

## Purpose

This procedure is used to connect to the CNFG host using the Provisioning GUI.

## Before you begin

### Related Information

You can also access the Provisioning GUI from the MI GUI.

Click the SNE. The **ManagedObjects menu** is displayed. From the **ManagedObjects menu**, select **Provisioning GUI**.

### Login account

Ensure that you have a login account to connect to the CNFG server (CNFG host).

### **SoftSwitchGUI.exe**

Ensure that you have downloaded *SoftSwitchGUI.exe* which is required to connect to the host. To download *SoftSwitchGUI.exe* perform the following:

1. Log in to MI OAM host as *lss*.
2. Change your directory to */opt/LSS/LMT/ProvGui*.  
`cd /opt/LSS/LMT/ProvGui`
3. Download the *SoftSwitchGUI.exe* to your local PC using FTP or SFTP.

## Procedure to connect to the CNFG host using the Provisioning GUI

Perform the following:

- 
- 1 Double-click *SoftSwitchGUI.exe*.

**Result:** The **Connecting to host** window is displayed.

---

- 2 In the **Name or IP address of the Host** field enter the IP address or name of the CNFG host.
  - 3 Click **Connect** to connect to the CNFG server.
-

**Result:** If the client versions match, the connection continues. If not, the **Client Download from <IP address/Name of Host>** screen is displayed with an error message.

- 
- 4 Enter the following information in the Client Download from <IP address/Name of Host> screen:

- **Name:** Enter the user name of the CNFG server.
- **Password:** Enter the password of the CNFG server.
- **Location:** This field provides the default location to download the client. You can change this location by clicking **Change** and selecting another location.

**Note:** Use the Linux login id and password in the **Name** and **Password** section.

The range of the fields are as follows.

- **Name:** 3 to 20 alphanumeric characters.
- **Password:** 3 to 19 alphanumeric characters.

- 
- 5 Click **OK** to download the client.

**Result:** If the download completes successfully, the following message is displayed:

Download completed successfully.

After the client is downloaded successfully, the client is launched to connect to the CNFG host.

**Note:** A maximum of three attempts are allowed to download the client. After the third failed attempt, the following message is displayed to the user:

Failed to download client. Max attempts (3) reached. Please download the client manually.

END OF STEPS

---

# To execute the base configuration

## Purpose

This procedure is used to execute the base configuration.

## Procedure to execute the base configuration

**Important!** Do not perform provisioning from the Provisioning GUI and the OMC-P during base configuration.

The base configuration tool adds SIPia ports and performs basic configuration.

Perform the following steps:

- 1 Log in to MI or CNFG host using external floating IP address and *lss* log in.

- 2 Execute the following command to stop the FS process:

```
FScmd stop fs vc
```

- 3 Log in to MI or CNFG host as *root*, execute the base configuration tool:

```
/export/home/root/bin/base_cfg.ksh 2>&1 | tee base_cfg.log
```

- 4 Log in to MI or CNFG host as *lss*, execute the following command to start the FS process:

```
FScmd start fs vc
```

- 5 **Note:** The services must be in the *InserviceActive* state or *InserviceStbyHot* state.

Log in to MI or CNFG host as *root*, execute the following command to query the status:

```
remSrvState -s ALL -d $(hostname)
```

- 6 Record the Shelf, Slot (Card), and Host of all cards with type 026 (IMS), 011 (H248) and 028 (5420 CTS) that are not in the *InserviceActive* state or *InserviceStbyHot* state.

- 7 If the cards do not change to the correct state after a while, reboot the hosts. For each host that is not *Inservice*, reboot the host from MI:

```
resetCard -s <shelf#> -c <card#> -h <host#>
```

- 
- 8 Wait for a few minutes for the local boot host or network boot host cards to come into service. Execute the following command to verify:

**remSrvState -s ALL -d \$(hostname)**

**Note:** If the cards do not enter the correct state, contact Technical Support.

---

- 9 Exit the procedure.

END OF STEPS

---

# To start and verify the FSDB

## Purpose

This procedure is used to start and verify the Feature Server Database (FSDB).

## Procedure to start and verify the FSDB

Perform the following steps:

- 1 Log in to MI or CNFG IP address of the SIP shelf as lss user.
- .....
- 2 Execute the **startMI** command to start the MI-Agent.
- .....
- 3 Execute the **startFS** command to start the FSDB service.
- .....
- 4 Execute the following command to ensure that all services are up and running:

**su - root**

You are prompted for a password. Enter the password for the root user.

- 5 Execute the following command:

**rccSrvState -d -r VM -s ALL**

**Result:** The status of the primary and alternate FSDB hosts is displayed.

- 6 Exit the procedure.

**E N D O F S T E P S**

# To provision NGSS Server parameters

## Purpose

This procedure is used to provision or modify the IMS Server (referred to as NGSS) parameters.

## Description

The IMS Server parameters include:

- ENUM IP Addresses
- Diameter application timers
- SIP session timers

*Note:* The NGSS Device Server is used as the base building block for providing other SIP-related services.

## Before you begin

### Points to remember:

The UDP/TCP switch depends on the following constraints:

- For Gm interface, if **SIP Gm UDP/TCP Switch** is enabled, and **Inhibit All SIP UDP/TCP Switch** is disabled, then the 5450 ISC performs SIP request switching. For other interfaces, if **Inhibit All SIP UDP/TCP Switch** is disabled, then the 5450 ISC performs SIP request switching.

If a request is within 200 bytes of the path MTU, or if it is larger than 1300 bytes and the path MTU is unknown, 5450 ISC sends the request using TCP if the other conditions are met.

- The switch function only works on SIP Request, not for the Response. The SIP response will follow the transport type of the corresponding request.
- If there is transport=parameter in Route header or R-URI.

## Steps to provision the NGSS Server parameters

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS → Parameters/Timers → NGSS Parameters**.

**Result:** The **NGSS Parameters/Timers** window is displayed.

**2**

| <b>If you want to...</b> | <b>then...</b>   |
|--------------------------|--|
| add NGSS parameters,     | Proceed with <a href="#">Step 3</a> .  |
| modify NGSS parameters,  | <ol style="list-style-type: none"> <li>1. Select the NGSS parameter to be modified.</li> <li>2. Enter the new value.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of procedure.</i></p> |

**3**

| <b>Parameter</b>                     | <b>Description</b>  |
|--------------------------------------|---|
| <b>Default Home Domain</b>           | In the <b>Default Home Domain</b> field, enter the Fully Qualified Domain Name that belongs to the IMS home network.  |
| <b>Enable Multiple Home Domains</b>  | Select the <b>Enable Multiple Home Domains</b> check box in case multiple home domains are required on a single Control Platform.   |
| <b>Authentication Realm</b>          | In the <b>Authentication Realm</b> field, enter the realm string used to authenticate the SIP request received on the NGSS server   |
| <b>Home I-CSCF</b>                   | <p>In the <b>Home I-CSCF</b> field, enter the I-CSCF SIP URI string.</p> <ul style="list-style-type: none"> <li>• When the <b>Home I-CSCF</b> is provisioned, the P-CSCF and S-CSCF insert this URI into the route header while processing requests that need to go to home I-CSCF</li> <li>• When the <b>Home I-CSCF</b> is NOT provisioned, a P-NAPTR lookup is done to find an I-CSCF.</li> </ul> <p><b>P-NAPTR configuration:</b></p> <p>No P-NAPTR lookup is done for the BGCF URI table, therefore the <b>Target URI</b> should include the Generic URI Label (GUL) and local domain zone (bgcf-stdn.east.example.com).</p> |
| The <b>ENUM Parameters</b> group box | <p>In the <b>ENUM Parameters</b> section, provision the following parameters:</p> <ul style="list-style-type: none"> <li>• In the <b>ENUM DNS Client Timeout(sec)</b> field specify the ENUM DNS Client time out (seconds) .</li> <li>• Select the <b>ENUM Query for Digits &gt; 18</b> check box to allow ENUM queries with digit count greater than 18 (up to 25 digits). This field is cleared by default.</li> </ul>  |
| <b>CX Timeout</b>                    | In the <b>CX Timeout</b> field, enter the time-out interval that the NGSS server must wait for a response from the HSS.   |

| Parameter   | Description   |
|---|---|
| <b>BGCF CIC Length</b>  | In the <b>BGCF CIC Length</b> field, enter the number of digits of the CIC.   |
| <b>Convert Display Digits from International to National format</b> | Select or clear the <b>Convert Display Digits from International to National format</b> check box (as desired).<br><br><b>Note:</b> If this check box is selected, and the country code in the CLI matches the country code in the <b>IMS &gt; Parameters/Timers &gt; Global Parameters</b> , then the terminating iAGCF converts the international format to the national format before forwarding the CLI to the end point. |
| <b>Enable VG Session and BW Control</b>                             | Select the <b>Enable VG Session and BW Control</b> check box to enable the session and bandwidth control for incoming and outgoing calls.   |
| <b>Generate Alarm for VG Session and BW Control</b>                 | Select the <b>Generate Alarm for VG Session and BW Control</b> check box to generate an alarm when calls are rejected after the maximum session/bandwidth limits are reached.   |
| <b>UE Re-registration for Geo-redundancy</b>                        | Select the <b>UE Re-registration for Geo-redundancy</b> check box to remove the stale registries from the P-CSCF.   |
| <b>IMS Core IP Version for Media Interworking</b>                   | Click <b>IPv4</b> or <b>IPv6</b> in the <b>IMS Core IP Version for Media Interworking</b> flag to determine the IP version to be used by the media (Service Description Protocol attachments and the Bearer Gateway).   |

| Parameter   | Description   |
|---|---|
| The <b>NP Parameters</b> group box                            | <p>Under <b>NP Parameters</b>,</p> <ul style="list-style-type: none"> <li>Select the appropriate option from the <b>Ported Parameter</b> list. When <b>1 - DN Ported</b> is selected, and the reply message for the ENUM query is either “E2U+pstn:tel” or “E2U+pstn:sip”, both I-CSCF and S-CSCF check if “ported = 1” exists as one of the TEL parameters, or as a part of the user name of the SIP URI. If it exists, the number is ported. <ul style="list-style-type: none"> <li>For the ported number, the I-CSCF rejects the call with error 410 and a reason header.</li> <li>For the ported number, the S-CSCF removes the “ported=1” parameter from the R-URI, and checks the value in the <b>QoR Prefix</b> field (specified in the next step). If it is not blank, the S-CSCF removes “+” (if present) from the dialed number, and prefixes it with the value in the <b>QoR Prefix</b> field. The S-CSCF also inserts a History Info header, if configured.</li> </ul> </li> <li>In the <b>QoR Prefix</b> field, enter the string to be applied as a prefix. Up to 15 characters are allowed in this field. This field can be left blank, if required.</li> </ul> |
| <b>SPDF Node-Functionality</b>                                | In the <b>SPDF Node-Functionality</b> field, enter the appropriate value to identify the Node-Functionality for the SPDF.   |
| <b>AGCF Node-Functionality</b>                                | In the <b>AGCF Node-Functionality</b> field, enter the appropriate value to identify the Node-Functionality for the AGCF.   |
| <b>S-CSCF relocation for geo-redundancy</b>                   | <p>Enable the <b>S-CSCF relocation for geo-redundancy</b> check box. When this check box is enabled, the S-CSCF provides a timer-based relocation procedure.</p> <p>The <b>S-CSCF relocation for geo-redundancy</b> check box can only be enabled when the <b>UE Re-registration for Geo-redundancy</b> check box is cleared.</p>   |
| <b>Minimum duration of registry before relocation attempt</b> | Enter the appropriate value in the <b>Minimum duration of registry before relocation attempt</b> field. This field defines the minimum duration between re-registration and the time when registry for the user is initially established, before relocation is attempted  |
| Click <b>Next &gt;</b> to go to the next screen.              |   |

| Parameter                                   | Description   |
|---|---|
| The <b>SIP Session Parameters</b> group box | <p>Under <b>SIP Session Parameters</b>, provision the following parameters:</p> <ul style="list-style-type: none"> <li>• Select <b>Enable</b> to enable the <b>SIP Session Timer</b>. The SIP session timer is used to refresh SIP sessions through a re-INVITE or UPDATE method. If the session is no longer active, the resources are released.</li> <li>• <b>Minimum Session Timer(sec)</b>, which is the minimum value for the session interval that the proxies are willing to accept.</li> <li>• <b>Session Expiration Timer(sec)</b>, which contains the desired heart-beating time interval.</li> </ul> |
| <b>Shortened Expiration Timer(sec)</b>      | In the <b>Shortened Expiration Timer(sec)</b> field, enter the time duration.Upon detection of S-CSCF loss of registry, the UEs registered with the affected S-CSCF have to be informed. The P-CSCF sends the NOTIFY messages to the affected UEs to shorten their registration time using the value defined in this field. The default value for this timer is 30 seconds.   |
| <b>SIP Next Hop Limit</b>                   | <p>In the <b>SIP Next Hop Limit</b> field, enter the per switch SIP next hop limit.</p> <p><b>Note:</b> This parameter is previously known as <b>P-NAPTR Retry Counter</b>.</p>   |
| <b>SIP Gm UDP/TCP Switch</b>                | <p>Click <b>Enable</b> to turn on or <b>Disable</b> to turn off the <b>SIP Gm UDP/TCP Switch</b>.</p> <p>The SIP Gm UDP/TCP switch function supports a switch from UDP to TCP when SIP messages using UDP reach 1500 bytes in length.</p>   |

| Parameter   | Description  |
|---|--|
| <b>SIP Alternate Route for SIP 503</b>                    | <p>Click <b>Enable</b> to turn on or <b>Disable</b> to turn off the <b>SIP Alternate Route for SIP 503</b> flag.</p> <p>When the <b>SIP Alternate Route for SIP 503</b> flag is enabled,</p> <ul style="list-style-type: none"> <li>• if a queried target returns 503 in response to INVITE, p-NAPTR attempts the next target in its provisioned list of targets, and re-sends the INVITE request to SIP stack with the next chosen target in the available list</li> <li>• if the queried record returns 503 in response to INVITE, SIP stack attempts the next record by re-sending the INVITE request to the next chosen record that is available</li> </ul> <p>When the <b>SIP Alternate Route for SIP 503</b> flag is disabled,</p> <ul style="list-style-type: none"> <li>• if a queried target returns 503 in response to INVITE, p-NAPTR sends the 503 response to the application that originated the request</li> <li>• if a queried record returns 503 in response to INVITE, the SIP stack sends the 503 response to the application that originated the request</li> </ul> <p>The <b>SIP Alternate Route for SIP 503</b> switch drives this behavior under the following situations:</p> <ul style="list-style-type: none"> <li>• The destination has multiple A/AAAA records</li> <li>• The pNAPTR has multiple targets</li> </ul> |
| <b>P-NAPTR Group Affinity</b>                             | <p>The <b>P-NAPTR Group Affinity</b> parameter is used to specify the maximum number of per-switch pNAPTR records to be tried in a group. Select a valid number for the <b>P-NAPTR Group Affinity</b> list.</p> <p>When set to “ALL”, all the records in a group per-switch are tried before moving to the next group.</p>   |
| <b>Percent of Users with Simultaneous TCP Connections</b> | <p><b>Note:</b> This parameter enables the support for symmetric TCP connections.</p> <p>In the <b>Percent of Users with Simultaneous TCP Connections</b> field, enter the percentage of users with simultaneous TCP connections.</p>  |
| <b>The Advanced Parameters</b> group box                  | <p>Under <b>Advanced Parameters</b>, provision the following parameters:</p> <ul style="list-style-type: none"> <li>• <b>ISUP To SIP Cause Code Mapping</b></li> <li>• <b>SIP To ISUP Cause Code Mapping</b></li> <li>• <b>ISUP Hop/SIP Forwards Ratio</b></li> <li>• <b>Redirect Timer.</b></li> <li>• <b>Send 100 Trying in response to non-INVITE request</b></li> <li>• <b>Immediately send 100 Trying in response to MESSAGE</b></li> </ul>   |

| Parameter   | Description  |
|---|--|
| The <b>Priority Parameters</b> group box                  | <p>Under <b>Priority Parameters</b>,</p> <ul style="list-style-type: none"> <li>• Select the <b>Priority Mode</b>. The Priority Mode specifies the priority mechanism to be used by the P-CSCF, I-CSCF, IBCF, and S-CSCF.</li> </ul> <p>If the priority mode is set to,</p> <ul style="list-style-type: none"> <li>– <b>NONE</b> - only emergency calls get priority treatment.</li> <li>– <b>CPC</b> - emergency and CPC priority calls get priority treatment.</li> <li>– <b>RPH</b> - emergency and GETS calls get priority treatment.</li> </ul> <ul style="list-style-type: none"> <li>• Select the <b>ets Value</b> list under <b>NGN GETS Parameters</b> to specify the ets priority value.</li> </ul> <p>The ets priority value is inserted in the RPH by the P-CSCF, I-CSCF, IBCF, and S-CSCF. The <b>ets Value</b> has five values, ets.0, ets.1, ets.2, ets.3, and ets.4. The default value is ets.0.</p> <p><b>Note:</b> This field is enabled only if the <b>Priority Mode</b> is set to <b>RPH</b>. When <b>Priority Mode</b> is set to <b>None</b> or <b>CPC</b>, the ets value is not used.</p> <ul style="list-style-type: none"> <li>• Under <b>NGN GETS Parameters</b>, in the <b>Feature Code</b> field, enter a feature code.</li> </ul> <p>Feature code should contain a leading “*” followed by three digits. The default is “*272”.</p> <p><b>Note:</b> The feature code is used only when the <b>Priority Mode</b> is set to <b>RPH</b>. When <b>Priority Mode</b> is set to <b>None</b> or <b>CPC</b>, the Feature Code is not used.</p> |
| <b>Wildcard PUID match for SIP URI without user=phone</b> | <p>Click <b>Yes</b> in the <b>Wildcard PUID match for SIP URI without user=phone</b> field to enable the CSCF to attempt to match the originating PUID (in SIP URI format, when the user portion is telephone number, but without user=phone) with the registered (and unregistered when applicable) wildcard PUID. This setting is useful when a PBX is not able to insert user=phone parameter using SIP URI format when the user=phone is needed.</p> <p><b>Note:</b> When this option is set to <b>No</b>, the CSCF does not attempt to match with a wildcard PUID.</p>  |
| <b>SIP Message Screening</b>                              | <p>Click <b>Enable</b> or <b>Disable</b> to enable or disable the <b>SIP Message Screening</b> flag.</p> <p><b>Note:</b> If you select <b>Enable</b>, a warning window is displayed. Click <b>Yes</b> to enable SIP message screening.</p>   |
| <b>Inhibit All SIP UDP/TCP Switch</b>                     | <p>Click <b>Yes</b> in the <b>Inhibit All SIP UDP/TCP Switch</b> flag to override UDP to TCP switching.</p>  |

| Parameter  | Description  |
|--|--|
| <b>Emergency RPH esnet Namespace Value</b>         | From the <b>Emergency RPH esnet Namespace Value</b> list, select the esnet priority value to be inserted in the RPH header. The esnet priority value is inserted in the RPH by the P-CSCF, I-CSCF, IBCF, iAGCF, and S-CSCF. The list has five values, esnet.0, esnet.1, esnet.2, esnet.3, and esnet.4.   |
| <b>Enable SIP next hop limit per SRV record</b>    | Select <b>Yes</b> to enable geo-redundancy using SRV RRs   |
| <b>Number of SRV records per Priority group</b>    | Select the maximum number of SRV records of the same priority level to be tried before moving on to the next set of SRV records with higher value of priority  |
| Click <b>Next &gt;</b> to go to the next screen.   |  |
| <b>Topology Hiding Host String</b>                 | <p>If required, change the value in the <b>Topology Hiding Host String</b> field. This value replaces the host portion of the headers affected by topology hiding.</p> <p><b>Note:</b> This field has to be necessarily populated when the field <b>SIP Topology Hiding</b> is enabled either in the P-CSCF profile or the IBCF profile.</p>   |
| <p>The <b>Media Inactivity Timer</b> group box</p> | <p>Under <b>Media Inactivity Timer</b>, enter the values for the following parameters:</p> <ul style="list-style-type: none"> <li>• <b>Audio/Image Media Inactivity Timer</b> - This value defines the recipient of two consecutive RA-Requests with Loss of Bearer Indication before the timer expires for Audio/Image media type. The default value is 180.</li> <li>• <b>Video Media Inactivity Timer</b> - This value defines the recipient of two consecutive RA-Requests with Loss of Bearer Indication before the timer expires for Video media type. The default value is 3600.</li> <li>• <b>Message Media Inactivity Timer</b> - This value defines the recipient of two consecutive RA-Requests with Loss of Bearer Indication before the timer expires for Message media type. The default value is 7200.</li> <li>• <b>Other Media Inactivity Timer</b> - This value defines the recipient of two consecutive RA-Requests with Loss of Bearer Indication before the timer expires for Other media type. The default value is 7200.</li> </ul> |
| <b>Support Wildcard PSI</b>                        | <p>Select the <b>Support Wildcard PSI</b> check box to enable the support of wildcarded PSI.</p> <p>If this check box is selected, then the S-CSCF and I-CSCF support the wildcarded PSI.</p>  |

| Parameter                                  | Description  |
|--|--|
| <b>Include P-Profile-Key</b>               | Select the <b>Include P-Profile-Key</b> check box to indicate if a P-Profile-Key header containing either wildcarded PSI or wildcarded PUID should be included when a request is forwarded to the next hop.  |
| <b>Relay Realm Status to AF</b>            | When the <b>Relay Realm Status to AF</b> check box is selected, the SPDF transfers realm status to P-CSCF/ALG. Prior to this option, the SPDF only kept tracking realm status by itself. This flag can only be changed from ‘Yes’ to ‘No’ if there are no SBLP profiles having field “Reject SIP Request when BGW Realm Unavailable” set to ‘Yes’.   |
| <b>Support SIP Heartbeat After failure</b> | This flag is used to determine if the SIP Link Manager starts the heart beat after a failed link is detected. An internal quarantine list is generated based on the heart beat results. The SIP stack checks this flag to determine if further action needs to be taken when a failure response is received from a request.  |
| <b>Enable Surrogate Registration</b>       | Select the <b>Enable Surrogate Registration</b> check box, to enable surrogate registration. This flag controls if Surrogate Registration is enabled or not. If this flag is off, you cannot configure any valid PBX table ID/index on P-CSCF SIPia port. If you want to switch off this flag, first ensure that there is no valid configured PBX table ID/index on P-CSCF SIPia port.                                 |
| The <b>S-CSCF Pool</b> group box           | Under <b>S-CSCF Pool</b> , provision the following parameters: <ul style="list-style-type: none"> <li><b>IMS Restoration Procedures</b> - Select the check box to use the IMS Restoration procedures defined in 3GPP 23.380 for the P-CSCF, SCSCF, and I-CSCF configured in the system</li> <li><b>S-CSCF Pool Mode</b> - Select the check box to indicate that the S-CSCF is working in a quasi-pool mode.</li> </ul> |

| Parameter  | Description  |
|--|--|
| The <b>Global Transport Preference Setting</b> group box | <p>Under <b>Global Transport Preference Setting</b>, select the values for the following parameters:</p> <ul style="list-style-type: none"> <li>• <b>UDP_Priority</b> - The default value is <b>Highest</b>. This field contains the preference of transports (UDP, TCP, or TLS) that will be used by an application to the core network <ul style="list-style-type: none"> <li>– when the transport cannot be determined by other means</li> <li>– or when the port is specified in the request or target URI</li> <li>– or when the request or target URI is numeric IP</li> </ul> </li> <li>• <b>TCP_Priority</b> - The default value is <b>Second Highest</b>. This field can be provisioned by an ordered list of one to three transports (UDP, TCP, or TLS), while there must be at least one transport in the check list.</li> <li>• <b>TLS_Priority</b> - The default value is <b>Not Present</b>. If the most preferred non-TLS transport is UDP, <ul style="list-style-type: none"> <li>– UDP will be used if the message size is less than or equal to 1300.</li> <li>– Next most preferred connection-oriented non-TLS transport (TCP), if present, will be used if the message size is larger than 1300 and switching to TCP is enabled.</li> </ul> </li> </ul> |
| <b>MSC Core Realm Id</b>                                 | Enter an appropriate value from the <b>MSC Core Realm Id</b> list. This field specifies the index to the Core_realm table. The “MSC core realm” is used by ATCF to reconfigure TEAR (adding a new termination that is associated with the target access leg to the existing context on the ATGW) during handover.  |
| <b>Domain Type for PANI</b>                              | From the <b>Domain Type for PANI</b> list, select the value that identifies the type of domain information that shall be included in the PANI header. The available options are sbc-domain, and access-domain which are internally represented as an integer (0 and 1).  |
| <b>IBC Enhanced GR</b>                                   | Select the check-box to enable the enhanced geo-redundancy for realm status change.  |
| <b>P-CSCF Pool Mode</b>                                  | Select the check-box to enable P-CSCF pool mode.   |
| <b>P-CSCF Pool Domain</b>                                | <p>P-CSCF pool domain is displayed. The P-CSCF pool domain is the right most domain name of the P-CSCF pool member FQDN.</p> <p>When P-CSCF handles UE registration request, it adds its URI in the format, GUL + Service Label + P-CSCF Pool Domain .</p> <p><b>Note:</b> To provision this parameter, ensure that the <b>P-CSCF Pool Mode</b> is enabled per LCP switch</p>  |

- 
- 4 Select **Finish** to save and close the window.

**Result:** The NGSS Parameters are provisioned successfully.

For more information on the NGSS Parameter descriptions, see the topic, **NGSS Parameters** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

---

# To provision an IMS Service association

## Purpose

This procedure is used to manage the association between an IP-Multimedia Subsystem (IMS) Service and the hardware (the host) that provides the service.

The IMS Service is a host that is used to provide SIP-related services.

*Note:* On the Provisioning GUI, the host that provides the IMS Service is referred to as the Next-Generation SIP Server (NGSS).

## Before you begin

The following constraints apply:

- If you want to create an association between the IMS Service and a redundant set of hosts:
  - A set of local boot or network boot host cards must have already been grown into the Alcatel-Lucent Control Platform
  - Verify if an IMS server exists already. If not, provision the IMS Server parameters and stack timers.
  - Verify if an IMS server exists already. If not, provision the IMS Server parameters. See “[To provision NGSS Server parameters](#)” (p. 10-9).
  - The **POOL TYPE** of the Processor cards must have been set to **ims**.
- Before you can delete an IMS Server, all related SIPia ports must have been removed and the server must have been taken out of service.

## Steps to provision an IMS Service association

Perform the following steps at the Provisioning GUI:

- 1 Click **System View** on the toolbar.

**Result:** The **System View** screen appears.

- 2 In the **System View** window, expand the **Services** node and then expand the **IMS** node.

| 3 | If you want to      | Then  |
|---|---------------------|---|
|   | add an IMS service, | <ol style="list-style-type: none"> <li>1. Select <b>IMS</b>.</li> <li>2. Right-click and select <b>Add an IMS service</b></li> <li>3. Continue with <a href="#">Step 4</a></li> </ol> |

| If you want to         | Then  |
|------------------------|---|
| modify an IMS service, | <ol style="list-style-type: none"> <li>Select the IMS service</li> <li>Right click, and select <b>Modify</b>.</li> <li>Change parameter values and click <b>Finish</b>.</li> </ol> <p><i>End of procedure.</i></p>  |
| delete an IMS service, | <ol style="list-style-type: none"> <li>Select the IMS service</li> <li>Right click and select <b>Delete</b>.</li> <li>Confirm deletion.</li> </ol> <p><i>Note:</i> Before the device server can be deleted, all the SIPia ports must have been removed.</p> <p><i>End of procedure.</i></p> |

- 4 On the **Service Configuration** window, a **Service Label Prefix** is generated but can be modified. Enter additional digits to create the service label.

- 5 Select **Add** under **Node Information**.

**Result** The **Add Blade(s)** window appears.

- 6 Enter the following under **Component Parameters**:

- LLC Node Id
- Pair Information
- Pool ID - Pool Name
- Service Label
- Web Portal Service Label

Enter the following under **Fixed Internal IP Address(es)**:

- IP Address 1
- IP Address 1

- 7 Select **OK**.

- 8 When the **Service Configuration** screen re-appears, fill in the remaining parameters and when completed enter **Finish**.

*End of procedure.*

- 
- 9 When the **Softswitch System Component Configuration** screen appears, alter either the **Reconnect After** or **Retry Count** fields.

Select **Next**.

---

- 10 Select **Finish**.

**Result:** The **Service Configuration** window reappears.

---

- 11 If required, modify the **Service Label Prefix** and select **Next**.

**Result:** The **Add Blade(s)** window reappears.

---

- 12 In the second screen of the **Softswitch System Component Configuration** window, the following parameters can be modified:

| Parameter       | Recommended provisioning |
|-----------------|--------------------------|
| Reconnect After | 001                      |
| Retry Count     | 03                       |

- 
- 13 Select **Next** and select **Finish** to modify the updated parameters.

*End of procedure.*

E N D O F S T E P S

---

# To provision a Diameter profile

## Purpose

This procedure is used to provision a Diameter profile.

## Description

The parameters that are specified in this profile are used by the Diameter protocol stack when the messages are sent over one of the application interfaces (for example, Rf, Cx, Sh, or Rx).

If there is an IMS, or Converged Telephony Server (CTS), to Diameter profile mapping and the Diameter profile contains either Cx or Rf connection interfaces, then the IMS or CTS establishes a direct Diameter Cx/Rf connection to HSS/CCF.

Before you create a Diameter port on an IMS service (for example, when you are adding a PD-FE), a Diameter profile *must* be assigned to that IMS service through a service-to-Diameter mapping.

## Diameter connection interface

The Diameter profile includes Diameter connection interfaces. The Diameter connection interfaces define the interfaces that are supported in the Diameter profile. For each interface connection, the type of Diameter application and the destinations are configured.

**Note:** In Diameter connection interface, provisioning the **Geographic Redundancy** and selection of **Multiple Destination Profile IDs** are mutually exclusive. That is, once the Geographic Redundancy configuration is provisioned then Multiple Destination Profile IDs are disabled and vice versa.

**Note:** Before you *delete* a Diameter profile, ensure that

- none of the application interfaces (for example Rf, Cx, Sh, or Rx) is operational
- all diameter profiles are deleted

## Steps to provision a Diameter profile

Perform the following steps at the provisioning GUI:

- 
- 1 Select **IMS → IMS Tables**.

**Result:** The **IMS Tables** screen is displayed.

---

- 2 In the left pane, expand **IMS → General**, and select **Diameter Profile**.

| 3 | If you want to...                       | then...   |
|---|---|---|
|   | add a <b>Diameter Profile</b> table,    | <ol style="list-style-type: none"> <li>Right-click <b>Diameter Profile</b> and select <b>Add Table</b>.<br/><b>Result:</b> The <b>Add Diameter Profile</b> dialog appears.</li> <li>Enter the Table Number and Table Name and click <b>OK</b>.</li> </ol> |
|   | rename a <b>Diameter Profile</b> table, | <p>do the following:</p> <ol style="list-style-type: none"> <li>Select the table you want to modify.</li> <li>Right-click and select <b>Rename Table</b></li> <li>Modify the name and click <b>OK</b>.</li> </ol> <p><i>End of procedure.</i></p>         |
|   | delete a <b>Diameter Profile</b> table, | <ol style="list-style-type: none"> <li>Select the table you want to delete.</li> <li>Right-click and select <b>Delete Table</b></li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of procedure.</i></p>                                 |

| 4 | If you want to... | then...  |
|---|-------------------|--|
|   | add a profile,    | <ol style="list-style-type: none"> <li>In the right pane, right-click and select <b>Add Table Attributes</b>.</li> <li>Go to <a href="#">Step 5</a>.</li> </ol>  |
|   | modify a profile, | <ol style="list-style-type: none"> <li>Select the profile you want to modify.</li> <li>Right-click and select <b>Modify Table Attributes</b>.</li> <li>Go to <a href="#">Step 5</a>.</li> </ol>  |
|   | delete a profile, | <ol style="list-style-type: none"> <li>Select the profile you want to delete.</li> <li>Right-click and select <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of procedure</i></p> |

5 Enter a **Profile ID**.

6 Type a unique (descriptive) name in the **Profile Name**.

- 7 Select the values for the three Dog Watch Request (DWR) related fields. Alcatel-Lucent recommends default values.
- 8 Select the values for the two CER related fields. Alcatel-Lucent recommends default values.

| 9 | If you want to...                              | then...  |
|---|--|--|
|   | add a Diameter Client Connection Interface,    | <ol style="list-style-type: none"><li>1. In the Diameter Connection Interface section, click <b>Add Client</b>.<br/><b>Result:</b> The <b>Diameter Connection Interface</b> window is displayed.</li><li>2. Go to <a href="#">Step 10</a></li></ol>  |
|   | add a Diameter Server Connection Interface,    | <ol style="list-style-type: none"><li>1. In the Diameter Connection Interface section, click <b>Add Server</b>.<br/><b>Result:</b> The <b>Diameter Server Interface</b> window is displayed.</li><li>2. Select the SCTP parameter profile to be assigned for the SCTP association in the <b>SCTP Parameter Profile</b> drop-down list.</li><li>3. Click <b>OK</b>.</li><li>4. Go to <a href="#">Step 24</a>.</li></ol>   |
|   | modify a Diameter Client Connection Interface, | <ol style="list-style-type: none"><li>1. In the Diameter Connection Interface section, select the client interface you want to modify.</li><li>2. Click <b>Modify</b>.<br/><b>Result:</b> <b>Diameter Connection Interface</b> window pops-up.</li><li>3. Go to <a href="#">Step 10</a></li></ol>  |
|   | modify a Diameter Server Connection Interface, | <ol style="list-style-type: none"><li>1. In the Diameter Connection Interface section, select the server interface you want to modify.</li><li>2. Click <b>Modify</b>.<br/><b>Result:</b> <b>Diameter Connection Interface</b> window pops-up.</li><li>3. Select the SCTP parameter profile to be assigned for the SCTP association in the <b>SCTP Parameter Profile</b> drop-down list.</li><li>4. Click <b>OK</b>.</li><li>5. Go to <a href="#">Step 24</a>.</li></ol> |

| If you want to...                                     | then...  |
|---|--|
| delete a Diameter Client/Server Connection Interface, | <ol style="list-style-type: none"> <li>1. In the Diameter Connection Interface section, select the interface (client/server) you want to delete.</li> <li>2. Click <b>Delete</b>.</li> </ol> <p><i>End of procedure.</i></p> |

## 10 Select an appropriate Application Type.

**Note:** The Diameter Connection Interface is for the Diameter services where the IMS service acts as a client. Only in 3GPP and 3GPP2, the PD-FE acts as a Sp' client. In TISPAN, the PD-FE acts as a Rq' client.

## 11 Configure the following Geographic Redundancy parameters:

| Parameter                    | Description  |
|------------------------------|--|
| <b>Destination FQDN</b>      | Enter the IP address of the application server in this field.<br><br><b>Note:</b> Either a FQDN host name or an explicit IP address is allowed in this field.                      |
| <b>Destination Port#</b>     | Enter the destination port number in this field.   |
| <b>Alt Destination FQDN</b>  | Enter the alternate IP address of the application server in this field (optional).<br><br><b>Note:</b> Either a FQDN host name or an explicit IP address is allowed in this field. |
| <b>Alt Destination Port#</b> | Enter the alternate destination port number in this field (optional).  |

### Notes:

1. If names are entered in the **Destination FQDN** and (optionally) **Alt Destination FQDN** fields, then click **DNS Look Up** to ensure that the DNS server is updated. For more information, refer to “[Refresh DNS entry](#)” (p. 10-30).
2. The port number entered in the **Destination Port** and (optionally) **Alt Destination Port** are for TCP and SCTP connections.
3. If the Diameter Multiple Destination Profile ID is selected, the Geographic Redundancy parameters will be disabled.
4. When **Destination FQDN** or **Alt Destination FQDN** is set to PD-FE FQDN or any other internal NI, diameter ignores the transport protocol configuration provisioned and always uses TCP as the transport protocol.

- 
- 12 Enter the minimum percentage of active connections in the **Min Percentage of Active Connections (%)** field.

**Note:** In case of Geographic Redundancy, the “Minimum Percentage of Active Connections (%)" is a percentage of total number of connections returned when DNS query is done for Primary Server FQDN and is used to calculate the number of minimum needed connections.

For Multiple Destination, the value of the “Minimum Percentage of Active Connections (%)" applies to all the FQDNs in the list. That is, the calculation of the minimum number of active DIAMETER connections is done separately for each FQDN based on the number of IP addresses returned from the DNS query. Therefore, for each FQDN the minimum number of active DIAMETER connections = ( number of query result for each FQDN ) \* ( provisioned percentage number).

In both the cases, if the resulted number is a fraction, then it will be rounded up to the nearest integer number. The value ranges from 1% to 100% in increments of 1%.

---

- 13 Check or uncheck the **Automatic DNS Query** field.

**Note:** If the Automatic DNS Query field is checked, then the Diameter stack automatically queries the DNS to get the server/service IPs after a specified time. The interval is based on the DNS query status and diameter connection status.

---

- 14 Select the required **Diameter Multiple Destinations Profile ID**.

**Note:** If the Geographic Redundancy parameters are entered, the Diameter Multiple Destination Profile ID field will be disabled.

**Note:** The Diameter Multiple Destinations Profile ID can be provisioned when the Application Type is set to Rx or Gq'. However, the Multiple Destination Profile that is associated with Rx and Gq' behaves differently since Rx and Gq' don't support "agent". It is recommended that the **agent** flag is not checked on the Multiple Destination profile, if the Multiple Destination profile is linked to Rx or Gq'.

---

- 15 In the **Min Percentage of Active Agent/Backup Connections[%]** field, enter the percentage of total number of connections returned when DNS query is done for the Primary FQDNs provisioned in the Diameter Multiple Destination Profile. It is used to calculate the number of minimum needed Primary connections. If the resulting number is a fraction, then it is rounded up to the nearest integer.

The default value is 50. The range is 1 to 100.

**16** Select the **DIAM over TCP** check box to support the TCP transport protocol.

**17** Select the **DIAM over SCTP** check box to support the SCTP transport protocol.

**Note:** If both **DIAM over SCTP** and **DIAM over TCP** check boxes are selected, the diameter connection (for client) tries the SCTP connection first and if the attempt fails, then it tries the TCP connection. If the TCP connection fails, the sequence is repeated till the connection is set up.

**18** Select the SCTP parameter profile to be assigned for the SCTP association in the **SCTP Parameter Profile** drop-down list.

**19** Configure the following DPR Parameters:

| Parameter                         | Description   |
|-----------------------------------|---|
| <b>DPR Message Timer (sec)</b>    | This field indicates the request message expiration timer value in seconds.<br><br>When a DPR message is sent, call processing starts a timer for the message. When the timer expires and no answer is received, call processing takes action based on the setting of “DPR Retransmission Maximum”.<br><br>When the DPR Message Timer is changed from “0” to a value greater than “0”, a warning message is printed: <i>“With a value greater than zero for DPR Message Timer field, deleting IP from DNS may result in going through DPR/DPA procedure first so that the connection will be torn down with a small delay.”</i> |
| <b>DPR Retransmission Maximum</b> | If the request message timer expires, <ul style="list-style-type: none"> <li>• 0 = No re-transmission required.</li> <li>• 1-10 = Number of re-transmissions.</li> </ul>  |

| Parameter                                   | Description  |
|---|--|
| <b>Re-connect Peer after Received a DPR</b> | <p>This field controls the Diameter Client whether or not it reconnects the peer from which a DPR was received.</p> <ul style="list-style-type: none"> <li>• Yes: Attempt to reconnect</li> <li>• No: Do not attempt to reconnect</li> </ul> <p>When this flag is changed from “Yes” to “No”, a warning message is printed: <i>“With this setting the Client will never try to reconnect the peer that previously sent a DPR message so the connection will be down forever after it is disconnected”</i>.</p> |
| <b>Re-connect Timer (sec)</b>               | <p>This field indicates the reconnect request message timer value in seconds, for a peer that previously sent a DPR message. When this timer expires, if the Re-connect peer is set to “Yes” after receiving a DPR flag, the client sends a transport connect request message to try to reconnect the peer. When the flag, <b>Re-connect Peer after Received a DPR</b> is changed from “Yes” to “No”, this field cannot be changed.</p>  |

- 20 Enter the value in the **DIAM DSCP** field. This field supports the provisioning of a DiffServ Code Point value for a particular Diameter interface. When this field is provisioned then the value is inserted into the appropriate field in the IP packet header.

**Note:** This field is grayed out if the transport type for the Diameter interface is only set to SCTP. If the transport type is set for both TCP and SCTP, then this field is allowed to be provisioned. This field is used for Client.

- 21 Enable the **Same origin-Host/Realm for CER and Application Message** check box to support a selection of using the same Origin-Host and Origin- Realm for both CER and Diameter Application messages. This field is applicable only for Rf, Ro and Rx interfaces. For other interfaces, this field is grayed out.

- 22 Select the **DNS Look Up** button.

When PDFE port is locked from the GUI, the connection between PDFE and PCSCF is disconnected. When again unlocked, the connection does not recover immediately and takes about an hour to come up. To recover it immediately, select DNS Look Up.

- 23 Click OK.

**Result:** The Diameter Connection Interface is added or updated.

- 24 Click OK.

**Result:** The profile is added or updated.

- 25 On the **IMS Tables** window, click **File > Save**.

**Result:** The changes are saved.

END OF STEPS

## Refresh DNS entry

Perform the following steps:

- 1 On the **Diameter Connection Interface** window, select an interface and click **Modify**.
- 2 Click **DNS Look Up**.

**Result:** The entry in the DNS server is updated.

**Important!** Applications use the FQDN to get a list of HSS/CCF IPs by querying the DNS.

To query the DNS for a list of host IPs:

1. Open the **Diameter Profile** window.
2. In the **Diameter Connection Interface** area of the window, double-click the desired application interface.
3. On the **Diameter Connection Interface** window, select the **Automatic DNS Query** check box.

**Result:** Diameter stack automatically queries the DNS to get the server/service IPs after a specified time. The interval is based on the DNS query status and diameter connection status.

END OF STEPS

# To modify Diameter application IDs

## Purpose

This procedure provides the steps to modify the application identifier (ID) table for the Diameter interfaces. The Diameter interfaces are used by the service components on the LCP.

The Diameter application ID table is downloaded to an IMS service when an IMS service is provisioned. After the IMS service is provisioned, the table is downloaded to each IMS service every time the table is modified.

## Related information

Each Diameter interface type is identified by an application ID (and a vendor ID). The set of application IDs for both the Diameter clients and the Diameter servers, is provisioned as an office-based table. Initially this table provides a default application ID for each Diameter interface type as proposed by the applicable standards (when the standard defines it). The operator can modify this table to specify another application ID to be used for a given interface. The change takes affect the next time a Diameter connection is set up.

The default values of the application IDs are inserted into the configuration database when the CNFG service starts up for the first time.

## Steps to modify Diameter application IDs

Perform the following steps at the Provisioning GUI:

- 1 On the **IMS** menu, select **Parameters/Timers** → **Diameter Application ID**.

**Result:** The **Diameter Application ID Parameters** dialog appears.

- 2 Modify the ID value for the desired Diameter application interface identifier.

- 3 Click **OK**

**Result:** The **Diameter Application ID Parameters** window is closed and the new data is saved in the configuration database.

END OF STEPS

# To provision a Service to Diameter mapping

## Overview

This topic describes the procedure to provision a **Service to Diameter mapping** table. The **Service to Diameter mapping** maps a service to a diameter profile.

A single **Service to Diameter mapping** table is defined. The table is used by IMS, 5420 CTS and Dual Mode Subscriber.

## Before you begin

Observe the following:

### Frequency

Perform this procedure whenever a Service to diameter mapping must be added, modified, or deleted.

### Required information



### NOTICE

#### Service-disruption hazard

*This procedure can be service affecting. During the conversion, all the Diameter connections will be torn down and the new connections will be re-established after the service to Diameter mapping is provisioned.*

*To minimize the service impact, the user needs to add the service to Diameter mapping for IMS or 5420 CTS one by one.*

If multiple destinations profile is used, then all the TCP/Diameter connections associated with the addresses of the entire Destination FQDN list will be pre-established. The user should check the status of the connections after the Service to Diameter mapping is provisioned.

Provisioning data to complete the procedure.

This procedure is performed at the FS GUI.

## Steps to provision a Service to Diameter Mapping table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS → IMS Tables**.

In the IMS tables window, navigate to one of the following folders:

- **IMS → General**
- **Dual Mode Subscriber (DMS) → General**
- **5420 CTS → General**

- 2 Expand the **Service to Diameter Mapping** folder.
- 3 Perform the following steps to add, rename, or delete a Service to Diameter mapping table.

| If you want to ...                          | then ...  |
|---|---|
| add a Service to Diameter mapping table,    | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>. Result: The <b>Add Service to Diameter mapping table</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <p><i>End of steps.</i></p> |
| rename a Service to Diameter mapping table, | <ol style="list-style-type: none"><li>1. Select <b>Tables → Rename Table</b>. Result: The <b>Rename Service to Diameter mapping table</b> window is displayed.</li><li>2. In the <b>Table Name</b> box, type a descriptive table name.</li><li>3. Click <b>OK</b>.</li></ol> <p><i>End of steps.</i></p>  |
| delete a Service to Diameter mapping table, | <ol style="list-style-type: none"><li>1. Select the table, and then select <b>Tables → Delete table</b>.</li><li>2. Click <b>Yes</b> to confirm deletion.</li></ol> <p><i>End of steps.</i></p>   |

- 4 Double-click the Service to Diameter mapping table. The Service to Diameter mapping table opens in the right pane. Perform the following steps to add, modify, or delete the Service to Diameter mapping table attributes:

| If you want to ...                    | then ...   |
|---------------------------------------|--|
| add a Service to Diameter mapping,    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The Service to Diameter mapping window is displayed.</li> <li>Continue with <a href="#">Step 5</a>.</li> </ol>   |
| modify a Service to Diameter mapping, | <ol style="list-style-type: none"> <li>Select a table entry.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The Service to Diameter mapping window is displayed.</li> <li>Continue with <a href="#">Step 5</a>.</li> </ol> <p><i>End of procedure.</i></p> |
| delete a Service to Diameter mapping, | <ol style="list-style-type: none"> <li>Select a table entry.</li> <li>Right-click and select <b>Delete Table Attributes</b>.</li> <li>Click <b>OK</b> to confirm deletion.</li> </ol> <p><i>End of procedure.</i></p>  |

- 5 Configure the following parameters:

| Parameters              | Description   |
|-------------------------|---|
| <b>Service Type</b>     | Select the service type.                                      |
| <b>Blade(s)</b>         | Select the blades associated with the service type.           |
| <b>Diameter profile</b> | Select the diameter profile associated with the service type. |

- 6 Click **OK**.

**Result:** The attributes are added or updated.

**Additional information:** For descriptions of the attributes, refer to *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

END OF STEPS

# IP session control

## Overview

### Purpose

This section contains common procedures for the IP Session Control. Some of these procedures are stand-alone procedures while the remaining are referenced from various procedures as a part of the provisioning task flows.

### Contents

|   |       |
|---|-------|
| To provision an SCTP Profile                                      | 10-37 |
| To provision a SIPia port   | 10-40 |
| To provision ENUM server addresses                                | 10-49 |
| To provision an incoming digit table                              | 10-50 |
| To provision the ENUM profile                                     | 10-57 |
| To provision an Originating Hosts list                            | 10-64 |
| Wildcards in digit strings  | 10-68 |
| To change the operational state of a host providing IMS Service   | 10-72 |
| To change the operational or administrative state of a SIPia port | 10-80 |
| To view the operational state of a host providing IMS Service     | 10-82 |
| To view the administrative state of a SIPia port                  | 10-83 |
| Verifying operational functionality using the ims_cli command     | 10-84 |
| To provision an External Domain Routing table                     | 10-99 |

# To provision an SCTP Profile

## Purpose

This procedure is used to provision an SCTP profile.

The purpose of creating different SCTP profiles is to match the near and far ends with the SCTP parameters for optimal performance.

**Note:** SCTP is not supported on the Gm interface (UE to P-CSCF).

Only *one* **SCTP profile table** is allowed and up to *eight* *profiles* can be created in the SCTP Profile table.

## Steps to provision a an SCTP Profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS → Global Tables**.

**Result:** The **Global Tables** window is displayed.

- 2 In the left pane, expand the **SCTP Profile** folder.

**Result:** The SCTP Profile tables are listed under the folder in the left pane.

If the folder is empty, add a SCTP Profile table.

Perform the following steps in the **Global Tables** window to add, rename, or delete a SCTP Profile table :

| If you want to ...        | then ...   |
|---------------------------|--|
| add a SCTP Profile table, | <ol style="list-style-type: none"><li>1. Select <b>Tables → Add Table</b>.<br/><b>Result:</b> The <b>Add SCTP Profile Table</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |

| If you want to ...           | then ...   |
|------------------------------|--|
| rename a SCTP Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename SCTP Profile Table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a SCTP Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><i>End of steps.</i></p>   |

- 3** Double-click the table to open the list of profiles defined for the table.

Add the SCTP Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4** **Note:** By default, the provisioning GUI has the **SCTP\_Param** table with a default Profile Id (zero).

Perform the following steps at the **Global Tables - SCTP Profile** window to add, modify, or delete the SCTP Profile table attributes:

| If you want to ...                     | then ...   |
|--|--|
| add the SCTP Profile table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>SCTP Parameters</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                      | then ...   |
|---|--|
| modify a SCTP Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>SCTP Parameters</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>Before modifying an SCTP profile, ensure that no SIP Linkset is using this profile, as all the SCTP associations using this profile are affected.</li> <li>For the modification to take affect, lock the SIP Linkset before modifying and then unlock.</li> </ul> |
| delete a SCTP Profile table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> <p><b>Note:</b> Before deleting an SCTP profile, ensure that no SIP Linkset is using this profile.</p>   |

- 5** For more information on the parameters, see the topic **SCTP Parameters** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 6** Click **OK**.

**Result:** The SCTP Profile table attributes are provisioned successfully.

END OF STEPS

# To provision a SIPia port

## Purpose

This procedure provides the steps to provision a SIPia port.

The SIPia port acts as a gateway between the SIP protocol stack and the software that runs on the hosts that provide the IMS Service. The total number of SIPia components of a given type, allowed on an IMS service is 256.

## Before you begin

Observe the following:

- Using the Provisioning GUI **System View**, a redundant pair of hosts must already have been associated with the IMS service.
- Ensure that the host pair has sufficient processing capacity required for a new SIPia port.
- Ensure that proper digital certification for the TLS Port number to function properly.

## Procedure

Perform the following steps on the Provisioning GUI:

- 1 On the toolbar, click **System View**.
- 2 In the **System View** window, expand the **Services** folder and then expand the **IMS** folder.
- 3 Expand the **IMS Service** folder for which you want to configure the SIPia port.
- 4 Double-click the **SIPia Port** to open the SIPia port configuration window.

| 5 | If you want to ...   | then ...  |
|---|----------------------|---|
|   | add a SIPia port,    | <ol style="list-style-type: none"> <li>1. Right-click in the SIPia port window and select <b>Add</b>.</li> <li>2. Continue with <a href="#">Step 6</a>.</li> </ol>            |
|   | modify a SIPia port, | <ol style="list-style-type: none"> <li>1. Select a SIPia port.</li> <li>2. Right-click and select <b>Modify</b>.</li> <li>3. Continue with <a href="#">Step 6</a>.</li> </ol> |

| If you want to ...   | then ...   |
|----------------------|--|
| delete a SIPia port, | <ol style="list-style-type: none"> <li>1. Select a SIPia port.</li> <li>2. Right-click and select <b>Lock</b>.<br/>Wait until the SIPia port is locked</li> <li>3. Right-click and select <b>Delete</b>.</li> <li>4. Click <b>OK</b> to confirm deletion</li> </ol> <p><i>End of procedure</i></p> |

**6****Note:**

- If the IMS node is associated to the IMUX, the Port Number must be unique across other IMS services in the same IMUX cluster and with the IMUX itself.
- The port cannot be deleted if the IMS Node exists in the IMUX to IMS Association table and the Port Name exists for the associated IMUX cluster in the IMUX Port table and it is the only IMS SIPia port with that port name or port type within the IMUX cluster.
- If the IMS node is associated to the IMUX, ensure that the IMS and IMUX ports are locked, before you delete IMS and IMUX SIPia ports.
- An IMUX service shall support up to 256 unique SIPia ports.

Configure the following parameters:

| Parameter        | Description  |
|------------------|--|
| <b>Port Type</b> | Select the port type for the SIPia port you want to provision.<br><br><b>Note:</b> This parameter cannot be modified.  |
| <b>Port Name</b> | Enter a port name in the following format:<br><br><b>&lt;xxxx&gt;-&lt;yyyy&gt;</b><br><br>xxxx - is a fixed identifier that identifies the port type.<br>yyyy is an additional identifier for the port.<br>For example: <b>PCSF-stdn</b> <sup>1</sup><br><br><b>Note:</b> This parameter cannot be modified. |

| Parameter          | Description  |
|--------------------|--|
| <b>Port Number</b> | <p>This is the non-secure IP port number used for SIP signaling with this SIPia port. The range excludes the IP port numbers used with IPsec. The known port numbers (other than 5060) must not be used.</p> <p>If the IMS node ID for the SIPia port is part of an IMUX cluster, the default is 15000 (or the next available port number starting from 15000).</p> <p>Valid range: [1024-32767]</p> <p>Default value: 5060.</p> <p>When the port is in a cluster, default value is 15000.</p> |

| Parameter                     | Description  |
|-------------------------------|--|
| <b>TLS Server Port Number</b> | <p>Enter the TLS server port number.</p> <p>To enter the TLS server port number, ensure that <b>Enable two NIs for SIP</b> is enabled.</p> <p>It is set to “” (NULL) by default. If set to “” (NULL), it indicates that the TLS server port is not configured currently.</p> <p>The TLS server port number must be:</p> <ul style="list-style-type: none"> <li>• same for any P-CSCF with the same Generic URI Label (GUL)</li> <li>• different from any other P-CSCF SIPia ports or other TLS server port numbers used by any other component within the same IMS service</li> </ul> <p>Once the TLS Port number entry is done, this field is disabled for any changes. However, the value “”(NULL) can be changed once.</p> <p>The range of valid port numbers is same as the port number entered.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• Valid TLS certificates must be installed for the TLS server port to open properly. After performing operations such as addition, modification, or deletion of the certificates, a switch-over of the impacted IMS service is required in order to apply the concerned changes to the certificate.<br/>For more information on certificate commands, see <i>Alcatel-Lucent 5400 Linux Control Platform Security Management Guide</i>, 270-702-015</li> <li>• A valid TLS software License (ITLSGm) is required to provision this field.</li> <li>• If a TLS server port is configured without a valid license, this field is reset to “” (NULL).</li> </ul> <p><b>Note:</b> The TLS server port is shared by Gm and Mw,</p> <ul style="list-style-type: none"> <li>• when <b>Interface Supports TLS</b> is set to Gm only, TLS server port listening on Gm interface.</li> <li>• When <b>Interface Supports TLS</b> is set to Gm and Mw, TLS server port listening on both Gm and Mw interfaces.</li> </ul> |

| Parameter                           | Description   |
|-------------------------------------|---|
|                                     | <p><b>Note:</b> The CA list must be installed for the TLS server port on Gm to open properly for the following two configuration deployments:</p> <ul style="list-style-type: none"> <li>• TLS is supported on <b>Gm only</b>, but <b>Enable Mutual Authentication</b> is checked on related mapping TLS profile.</li> <li>• or TLS is supported on <b>Gm+Mw</b>.</li> </ul> <p><b>Note:</b> When the TLS server port is set to one valid non-zero value, there will be one cross check to ensure that the <b>Interface Supports TLS</b> is set to either <b>Gm only</b> or <b>Gm+Mw</b>.</p> |
| <b>Port Profile</b>                 | <p>Select a profile you provisioned, after the SIPia port is configured.<sup>2</sup></p> <p><b>Note:</b> The port profile cannot be reassigned while the port is in service. To change the assigned profile, lock the SIPia port before changing the profile and then unlock it.</p>  |
| <b>Member of External GUL Group</b> | <ul style="list-style-type: none"> <li>• Retain <b>Yes</b> if the SIPia port's SRV (ARRs) must be accessible from a remote DNS server.</li> <li>• Select <b>No</b> if the SIPia port's SRV (ARRs) must not be accessible from a remote DNS server.</li> </ul>   |
| <b>Global Port Identifier</b>       | <p>A unique system generated number is assigned to this field if the <b>Port Type</b> is P-CSCF.</p> <p><b>Note:</b> This field is not configurable.</p>  |
| <b>ACR Messages Generation</b>      | <p>Select the check box to enable ACR messages generation.</p> <p>For more details, see “<a href="#">To activate an ACR message generation on a SIPia port</a>” (p. 8-3).</p> <p>For more details, see <i>Alcatel-Lucent 5450 IP Session Control Provisioning Guide</i>.</p>  |

| Parameter                                 | Description  |
|---|--|
| <b>Enable Two NIs for SIP</b>             | <p>Select the check box to enable two network interfaces.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• This field is available for provisioning for P-CSCF port types only.</li> <li>• This field is checked and grayed for all IBCF SIPia ports.</li> <li>• This field is unchecked and grayed for the other port types.</li> <li>• This field is checked when a TLS Server Port is configured.</li> <li>• This field cannot be modified after the SIPia port is configured.</li> </ul>   |
| <b>PBX Table ID</b>                       | <p>This field defines the PBX Table (identified by PBX Table ID) used by a P-CSCF instance when the P-CSCF instance (that is, SIPia Port) is configured.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• When the “Enable Surrogate Registration” option in the NGSS parameter is disabled, the user cannot configure valid PBX table ID or index except “0” or “None”.</li> <li>• If there is a valid PBX Table ID or index configuration, the “Enable Surrogate Registration” option in the NGSS Parameter cannot be disabled.</li> </ul> |
| <b>SIP Permanent Linkset Group Number</b> | <p>This field is disabled for BGCF, LIFC, DTAS, GTAS and STAS SIPia port types and is enabled for all other Port types.</p> <p><b>Note:</b> Configuring this parameter is optional for enabling the support of two network interfaces for SIP communication.</p>   |
| <b>Area ID</b>                            | <p>This parameter used by the P-CSCF to populate the X-ALU-Area-ID parameter sent to the S-CSCF during UE registrations.</p> <p>The default value is zero and is not available for non-P-CSCF port types.</p>  |

| Parameter                                     | Description   |
|---|---|
| <b>NTM Control Table</b>                      | <p>This field is applicable to P-CSCF, I-CSCF, IBCF and iAGCF. An update of this field in P-CSCF, I-CSCF, IBCF and iAGCF port is applied across all blades that have the same port name and port type.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• This field is allowed for provisioning only when a proper NTM license is installed.</li> <li>• An NTM table needs to be created before assigning it to a SIPia port.</li> <li>• The table ID zero means that NTM is disabled.</li> <li>• Configuring this parameter is optional, for enabling the support of two network interfaces for SIP communication.</li> </ul> |
| <b>NTM Exemption for Authorization Header</b> | <p>When the Authorization or Proxy-Authorization Header is present in the SIP message and this field is checked, the Request is exempted from NTM.</p> <p><b>Note:</b> This field is available for P-CSCF, IBCF and I-CSCF Port Types. This field can be checked, only when a valid NTM Control Table Id is provisioned.</p>  |
| <b>Include NTM Proprietary AVP</b>            | <p>If this field is checked, the NTM while sending an ACR will include the proprietary AVP containing the control information.</p> <p>When this field is unchecked, the NTM will not include the AVP specific to the NTM.</p> <p><b>Note:</b> This field is available for P-CSCF and IBCF Port Types. This field can be checked, only when a valid NTM Control Table Id is provisioned.</p>   |
| <b>IPv4 Subnet</b>                            | <p>The SIP stack compares the entry in this field with the Subnet of the source IPv4 address, of the inbound SIP traffic. If there is a match, then the SIP stack continues with the message processing. If it does not match, then the SIP message is dropped.<sup>4</sup></p>   |

| Parameter                                  | Description  |
|--|--|
| <b>IPV4 Mask</b>                           | <p>This field specifies the number of times “1” is used contiguously, to build the IP mask. The remaining space is completed with contiguous “0” to complete the 32 bits when applying the mask.</p> <p>This IP mask is applied to the source IPv4 address of the inbound SIP traffic.</p>   |
| <b>IPV6 Subnet</b>                         | <p>The SIP stack compares the entry in this field with the Subnet of the source IPv6 address, of the inbound SIP traffic. If there is a match, then the SIP stack continues with the message processing. If it does not match, then the SIP message is dropped.</p>  |
| <b>IPV6 Mask</b>                           | <p>This field specifies the number of times “1” is used contiguously, to build the IP mask. The remaining space is completed with contiguous “0” to complete the 128 bits when applying the mask.</p> <p>This IP mask is applied to the source IPv6 address of the inbound SIP traffic.</p>  |
| <b>STN-SR ID</b>                           | <p>This field specifies the index to the STN-SR Identifier provisioned in the STN-SR Table.</p> <p>See <sup>6</sup></p>  |
| <b>Support SIP Heartbeat After failure</b> | <p>This field determines if the specific SIPia port supports the SIP Link Manager HB after a failed link is detected. The operator can select the specific component(s) of interest for monitoring the unavailable links.</p> <p>It is applicable for P-CSCF, S-CSCF, I-CSCF, BGCF, E-CSCF and AGCF. This flag can only be enabled if the global support SIP Heartbeat after failure is enabled.</p> |

**Notes:**

1. Using **stdn** in the port name is a recommendation and not a requirement.
2. In FEPH scenario this field maps to the P-CSCF profile record. If the IMS service has FEPH enabled, the P-CSCF port profile must have the Security Gateway ID specified and the Security Gateway profile must have the FEPH policy Ids specified (non-zero). If the IMS service does not have FEPH enabled and the P-CSCF port profile has the Security Gateway ID specified, the Security Gateway must have the FEPH policy Ids unspecified (set to zero). You cannot create an IBCF SIPia port on an IMS service that has FEPH enabled.

3. To enable the support of 2 network interfaces for SIP communication on an existing P-CSCF, the P-CSCF must be deleted from every IMS service and completely removed before enabling the **Enable Two NIs for SIP** parameter and re-configuring the P-CSCF.
4. To configure the Security IP filtering Subnet and Mask, ensure that the **Enable Two NIs for SIP** check box is selected.
5. The Security IP Filtering Mask for Inbound Traffic fields (IPv4 Subnet, IPv4 Mask, IPv6 Subnet, IPv6 Mask) are enabled for AGCF SIPia ports. The **Enable Two NIs** field is disabled for AGCF SIPia ports.
6. The **STN-SR ID** field is available for P-CSCF SIPia Ports only. The same STN-SR ID cannot be shared among IMS services. The STN-SR can be shared by P-CSCFs on the same IMS service, but will have to be unique per IMS service. The **Support ATCF** field on the P-CSCF profile can be enabled only if the Port has a non-zero STN-SR ID provisioned. The **Support ATCF** field on the profile in-use can be updated only if the Port is LOCKED. The **STN-SR ID** field on the port can be updated only if the Port is LOCKED. This also means that for a given STN-SR entry that is being used on the port, modifications to the STN-SR identifier value are allowed only if the Port is LOCKED.

For other parameters, retain the default values (recommended) or use a value that is required for your network.

- 7 Click **OK**.
- 8 Select the SIPia you created.
- 9 Right-click and select **Unlock** to enable the SIPia port.
- 10 Click **Yes** to confirm the unlock operation.
 

**Note:** You need not unlock the port when changing NTM control table or profile.
- 11 From the menu bar, select **File → Exit** to close the System View window.

END OF STEPS

# To provision ENUM server addresses

## Purpose

This procedure is used at the MI-Agent to provision the ENUM server address used during Interrogating Call Session Control Function (I-CSCF), to process calls.

## Procedure

Perform the following steps at the MI GUI:

- 
- 1 At the MI GUI, navigate to **Configuration Management > ENUM**.

**Result:** The current values are displayed.

---

- 2 Edit any of the fields to update one or all the four parameters( ENUM Domain and three IP addresses) displayed.

.

---

- 3 To enact, select **Modify** or select **Refresh** to return to original settings (no change made).

**Result:** A Confirmation window opens. If confirmed, the changes take place, otherwise the screen is refreshed.

ENUM Server domain can only be added or updated and not deleted. ENUM server IP addresses can be added, deleted, or updated using the **Modify**. Modification takes a few minutes. During that time no other operation can take place on this ENUM screen.

END OF STEPS

---

# To provision an incoming digit table

## Purpose

This procedure is used to provision an incoming digit table attributes.

## Description

Incoming digit tables are used for incoming digit matching and translation, service selection, error detection, and emergency number identification for digit strings on an incoming span or channel.

## Before you begin

The digit table must exist under **Incoming Digit Table**.

### Required information

You need to know the following:

- The type of digit table operation you want to perform
- The type of string to match
- The string to match.

## Steps to provision an Incoming Digit table

Perform the following steps at the Provisioning GUI:

- 
- 1 On the tool bar, click **Digit Table**.

**Result:** The **Digit Tables** window is displayed.

---

- 2 In the left pane, expand the **Incoming Digit Table** folder.

**Result:** The Incoming Digit tables are listed under the folder in the left pane.

If the folder is empty, add an Incoming Digit table.

Perform the following steps in the **Incoming Digit Table** window to add, rename, or delete an Incoming Digit table :

| If you want to ...              | then ...  |
|---------------------------------|---|
| add an Incoming Digit table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Digit Table Designation</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename an Incoming Digit table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Digit Table Designation</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |
| delete an Incoming Digit table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an Incoming Digit table, ensure that no table entries are in use.</p> <p><i>End of steps</i></p>   |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the Incoming Digit table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **Digit Tables** window to add, modify, or delete the Incoming Digit table attributes:

| If you want to ...                         | then ...  |
|--|---|
| add the Incoming Digit table attributes,   | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Incoming Digit Table attributes</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify an Incoming Digit table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Incoming Digit Table attributes</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete an Incoming Digit table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>                               |

- 5 Provision the following parameters:

| Parameter                    | Provisioning   |
|------------------------------|--|
| <b>Enable</b>                | Select <b>Yes</b> .  |
| <b>Digit Table Operation</b> | Select one of the following options:                                       |
| Wireless Translation         | Results in a lookup in the HLR, normally with the mobile subscriber number |

| Parameter              |                                   | Provisioning  |
|------------------------|-----------------------------------|---|
|                        | Translation                       | Translates a matched string and/or associated call parameters to a different digit string and parameters  |
|                        | TLDN Translation                  | Translates a matched string into a temporary local directory number (TLDN).   |
|                        | Local MSRN Translation            | Results in a lookup in the VLR, normally with the roaming number  |
|                        | Local MSRN Remote MSC Translation | Local Mobile Station Routing Number (MSRN) for remote MSC translation.  |
|                        | Remote MSRN Translation           | Remote Mobile Station Routing Number (MSRN) translation.  |
|                        | Local HO Translation              | Results in a translation of the specified digit string  |
|                        | Emergency Number                  | Identifies a digit string as an emergency number  |
|                        | Error Detection                   | Identifies a digit string that represents an error condition and assigns an appropriate cause code  |
|                        | Service Selection                 | Invokes the selected subscriber service.  |
|                        | Wrls Priority Service Selection   | Invokes the Wireless Priority Service. A specified feature code (*272) is read by the MSC and which provides priority service to authorized users during disasters. |
|                        | WPS Translation                   | Results in a translation of the specified digit string (*272) for Wireless Service Priority.  |
| <b>String to Match</b> |                                   | Select Dialed Number.<br>The following are the available options:   |
|                        | Carrier Number                    | Identifies the carrier that is associated with the incoming call  |
|                        | Dialed Number                     | Called party number   |
|                        | Originating Line Info             | Identifies the Automatic Number Identification (ANI) II source of the incoming call   |
|                        | Originating Number                | Calling party number.   |

| Parameter                                    | Provisioning  |   |
|--|---|---|
| <b>String</b>                                | <p>Type the digit string to be translated.<br/>Wild cards can be used</p> <p>See “<a href="#">Wildcards in digit strings</a>”<br/>(p. 10-68)</p>  |   |
| <b>Operations</b>                            | <p>If this section is highlighted, select the appropriate value(s).</p> <p><b>Result:</b> In this group you specify the type of operation that the digit table performs, as well as the string and parameters that the DPE uses for digit matching. The available parameters are based on the type of operation you select.</p> |   |
| <b>Map Protocol</b>                          | <p>This field is available only if the <b>Digit Table Operation</b> type is <i>Wireless Translation</i>.</p> <p>This field specifies the type of HLR query. Select one of the following:</p>  |   |
|  | GSM MAP   | Call uses GSM MAP. There is no retry if the attempt fails             |
|  | GSM Retry   | Call starts with GSM MAP, and if this fails, will retry with ANSI-41  |
|  | ANSI-41   | Call uses ANSI-41. There is no retry if the attempt fails             |
|  | ANSI-41 Retry   | Call starts with ANSI-41, and if this fails, will retry with GSM MAP. |
| <b>Secondary String Used For Translation</b> | <p>If this group is available, select appropriate values</p> <p><b>Result:</b> In this group you specify a wildcard string that the DPE can use in conjunction with the translation strings to translate a billing number, carrier number, dialed number and/or originating number.</p>   |   |

| Parameter                       | Provisioning  |
|---------------------------------|---|
| <b>Call Characteristics</b>     | <p>If this group is available, select appropriate values</p> <p><b>Result:</b> In this group you can assign priority, type and access level values to emergency number, service selection and translation-related calls.</p>  |
| <b>Error Detection</b>          | <p>If this group is available, select appropriate values</p> <p><b>Result:</b> In this group you can specify the cause code that the DPE associates with the dialed number or the carrier number that represents an error condition.</p>  |
| <b>Translation</b>              | <p>If this group is available, select appropriate values</p> <p><b>Result:</b> In this group you can specify the digit strings and parameters that the DPE uses to translate incoming digit strings and their parameters.</p>   |
| <b>Action After Translation</b> | <p>If this group is available, select appropriate values</p> <p><b>Prefix NPA</b> — When checked, results in a mobile originated call are being treated as though the user dialed &lt;mobile's&gt; NPA+XXX-YYYY. This functionality will only work when the digit string is exactly seven digits (with no ‘&amp;’ in it), and the Country Code in MSC Parameters screen is set to 1 (National).</p> <p><b>Re-run Digit Table</b> — Specifies whether the DPE (Dialing Plan Engine) is to repeat the digit matching process for the translated string. Selecting “None” indicates to not perform this action. Selecting the desired digit table from the pull-down menu re-runs the DPE engine for that table.</p> |

| Parameter                                       | Provisioning  |
|---|---|
| <b>Location Based Dialed Number Translation</b> | <p>Select <b>On</b> to enable the translation of the called party number based on the geographical area (location) of the calling party</p> <p>Under <b>Translation</b>, the <b>Dialed # Translate</b> box and the <b>Dialed # Indicator Nature of Address</b> fields are unavailable.</p> <p>This provisioning is available when:</p> <ul style="list-style-type: none"> <li>• <b>Digit Table Operation</b> is set to <b>Emergency Number, Service Selection</b>, or <b>Translation</b></li> <li>• <b>String To Match</b> is set to <b>Dialed Number</b>.</li> </ul> |
| <b>Service Selection</b>                        | <p>If this group is available, select appropriate values</p> <p>In this group you specify the subscriber service that the DPE invokes for the matched digit string.</p>   |
|   |   |

For more information on the parameters, see the topic **Incoming Digit Table attributes** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 6 Click **OK**.

**Result:** The Incoming Digit table attributes are provisioned successfully.

END OF STEPS

# To provision the ENUM profile

## Purpose

This procedure is used to provision the ENUM profile.

## Before you begin

Ensure that the ENUM profile ID is provisioned in the S-CSCF profile.

## Steps to provision a ENUM Profile table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Tables**.

**Result:** The **IMS Tables** window is displayed.

- 2 In the left pane, expand the **IMS** folder, then the **General** folder, and then the **ENUM Profile** folder.

**Result:** The ENUM Profile tables are listed under the folder in the left pane.

If the folder is empty, add a ENUM Profile table.

Perform the following steps in the **IMS Tables - ENUM Profile** window to add, rename, or delete a ENUM Profile table :

| If you want to ...        | then ...  |
|---------------------------|---|
| add a ENUM Profile table, | <ol style="list-style-type: none"><li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add ENUM Profile table</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |

| If you want to ...           | then ...   |
|------------------------------|--|
| rename a ENUM Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename ENUM Profile table</b> window is displayed.</li> <li>In the <b>Table Name</b> box, type a new table name.</li> <li>Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a ENUM Profile table, | <ol style="list-style-type: none"> <li>Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete a ENUM Profile table, ensure that no table entries are in use.</p> <p><i>End of steps.</i></p>                  |

- 3 Double-click the table to open the list of profiles defined for the table.  
Add the ENUM Profile table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.
- 4 Perform the following steps at the **IMS tables - ENUM Profile** window to add, modify, or delete the ENUM Profile table attributes:

| If you want to ...                     | then ...  |
|--|---|
| add the ENUM Profile table attributes, | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>ENUM Profile</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                      | then ...  |
|---|---|
| modify a ENUM Profile table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>ENUM Profile</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete a ENUM Profile table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>2. Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>3. Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p>            |

**5** Provision the following parameters:

| Parameter         | Provisioning          |
|-------------------|-----------------------|
| <b>Profile ID</b> | Select the profile ID |

| Parameter                         | Provisioning  |
|-----------------------------------|---|
| <b>ENUM Query For All Domains</b> | <p>Select <b>Yes</b>, if the S-CSCF should make an ENUM query regardless of the value in the host part of the SIP URI</p> <p><b>Note:</b> If the field is selected, the ENUM query is made for a UE originated request where the user part of the SIP URI contains digits or a user=phone parameter, and regardless of whether the S-CSCF owns the domain name in the host part of the SIP URI.</p> <p>If the field is not selected, the ENUM query is made for a UE originated request where the user part of the SIP URI contains digits and the S-CSCF owns the domain name in the host part of the SIP URI. If the URI is a SIP URI where the host portion contains a domain name that is not owned by this S-CSCF, the S-CSCF will send the request to the IBCF or I-CSCF.</p> |
| Bypass ENUM Query If CIC Present  | <p>Select <b>Yes</b> to enable an ENUM query if the Request-URI contains a cic parameter.</p> <p>If this field is set to "yes" and the Request-URI contains a "cic" parameter, the RTCF adds a Route header with the configured "BGCF Host URI" and forward the request based on the Route header.</p> <p><b>Note:</b> The RTCF (as a component) cannot be provisioned starting R20.0. The functions performed by the RTCF have been merged into the I-CSCF. However, the I-CSCF can be provisioned to perform the RTCF functionality.</p>  |

| Parameter                             | Provisioning  |
|---------------------------------------|---|
| ENUM Query When Digits In SIP URI     | <p>If this field is set to “yes”, then the S-CSCF performs an ENUM query for a UE originated request if the SIP URI in the Request-URI has digits in the user part.</p> <p>If “no” is selected, the S-CSCF performs an ENUM query only when the SIP URI in the Request-URI contains a user=phone parameter.</p> <p>In order for the ENUM query to made in either case, the host part of the SIP URI has to be owned by the S-CSCF or the ENUM Query for All Domains option has to be set to “yes.”</p>  |
| ENUM Query When Hex Digits in SIP URI | <p>If set to “yes”, then S-CSCF or RTCF considers making ENUM query for SIP request if SIP URI in the Request-URI has hexadecimal digits in the user part. This option is set to “yes” for SIP URI without the “user=phone” parameter.</p> <p>If set to “no”, S-CSCF or RTCF only considers making ENUM query when SIP URI in the Request-URI has “user=phone” parameter or if “ENUM Query when Digits in SIP URI” is set to “yes”. ENUM query is performed for TEL URI regardless of the setting of this flag.</p> <p><b>Note:</b> The RTCF (as a component) cannot be provisioned starting R20.0. The functions performed by the RTCF have been merged into the I-CSCF. However, the I-CSCF can be provisioned to perform the RTCF functionality.</p> |
| ENUM Supports Hex digits              | <p>If set to “yes”, this indicates if queries should be sent to ENUM server using hexadecimal digits (if yes), or only for decimal digits (if no).</p> <p>If set to “no”, this indicates if queries should be sent to ENUM server only for decimal digits.</p>  |

| Parameter                          | Provisioning   |
|------------------------------------|--|
| Bypass ENUM Query If NPDI Present  | <p>If set to Yes, this indicates that the ENUM query is bypassed when 'npdi' indication is present in the Request-URI.</p> <p>If set to No, this indicates that the ENUM is queried irrespective of whether 'npdi' indication is present or not.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• This field is applicable only to I-CSCF, and not to S-CSCF.</li> <li>• For a newly created ENUM profile, this field can be set to Yes or No. However, for the ENUM profile which is already associated with an I-CSCF profile, it can be set to Yes, only when the Address Resolution Method field in the associated I-CSCF profile is configured as one of the following: Cx before ENUM, or ENUM before Cx, or Cx only.</li> </ul> |
| Bypass ENUM Query for Local Number | <p>If set to "yes", then ENUM query will not be performed for numbers considered to be Local numbers.</p> <p><b>Note:</b> This field controls whether the ENUM query should be bypassed when the Request-URI contains a phone context parameter. If the phone-context parameter is received in the R-URI, the DA function will be bypassed. If the phone-context parameter is received, then the DA function will not remove the phone-context parameter. This field is set to "yes" by default.</p>   |
| <b>Call Type Based ENUM Query</b>  | <p>Yes/No</p> <p>Default: No</p>   |
| <b>Check (x-)enumdi</b>            | <ul style="list-style-type: none"> <li>• enumdi</li> <li>• x-enumdi</li> </ul> <p>Default: enumdi</p>  |

**Note:** The maximum number of ENUM profiles allowed in the system is 32.

For Rel26, the **Call Type Based ENUM Query** field is set to **No** and is disabled on GUI. A check will be added in the Xml interface to not allow the user to set this field to Yes.

---

For more information on the parameters, see the topic **ENUM Profile** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

---

- 6 Click **OK**.

**Result:** The ENUM Profile table attributes are provisioned successfully.

END OF STEPS

---

# To provision an Originating Hosts list

## Purpose

This procedure is used to provision an Originating Hosts list.

## Steps to provision a Originating Host List table

Perform the following steps at the Provisioning GUI:

- 1 Select **IMS** → **IMS Tables**.

**Result:** The **IMS Tables** window is displayed.

- 2 In the left pane, expand the **IMS** folder, then the **General** folder, and then the **Origination Host List** folder.

**Result:** The Origination Host List tables are listed under the folder in the left pane.

If the folder is empty, add a Origination Host List table.

Perform the following steps in the **IMS Tables** window to add, rename, or delete a Origination Host List table :

| If you want to ...                    | then ...   |
|---------------------------------------|--|
| add a Origination Host List table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add Orginating Host List table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename a Origination Host List table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename Orginating Host List table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |

| If you want to ...                    | then ...  |
|---------------------------------------|---|
| delete a Origination Host List table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an Originating Host list, ensure that there are no Originating Hosts lists used by the I-CSCF profile.</p> <p><i>End of steps.</i></p> |

**3** Double-click the table to open the list of profiles defined for the table.

Add the Origination Host List table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

**4** Perform the following steps at the **IMS Tables** window to add, modify, or delete the Origination Host List table attributes:

| If you want to ...                               | then ...  |
|--|---|
| add the Origination Host List table attributes,  | <ol style="list-style-type: none"> <li>1. Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Originating Host Details</b> window is displayed.</li> <li>2. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>   |
| modify a Origination Host List table attributes, | <ol style="list-style-type: none"> <li>1. In the right pane, select the profile that you want to modify.</li> <li>2. Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Originating Host Details</b> window is displayed.</li> <li>3. Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |

| If you want to ...                               | then ...   |
|--|--|
| delete a Origination Host List table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete. To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes → Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps.</i></p> |

**5** Provision the following parameters:

| Parameter          | Provisioning  |
|--------------------|---|
| <b>Host Type</b>   | Select the host type to indicate the format of the host name<br><br>Select one of the following options: <ul style="list-style-type: none"> <li>• Domain</li> <li>• IPv4 Address</li> <li>• IPv6 Address</li> </ul>   |
| <b>Host Name</b>   | Type either the Domain or the IP address of the host name in accordance with the selection made in the Host Type field.   |
| <b>Subnet Mask</b> | Type the range of the IP address<br><br>The IP address range is required for matching the ranges of the IP addresses, as wildcard characters are not supported for IPv6 addresses.  |
| <b>Class</b>       | Specify the Originating Host Traffic Class that will be used by BGCF for routing purpose.<br><br>I-CSCF uses this entry to populate a lu-ohclass parameter. If it is not populated, then Class routing treatment for the request does not apply for the originating host. |

| Parameter                  | Provisioning   |
|----------------------------|--|
| <b>Route based on CgPN</b> | Select Yes to configure I-CSCF to support routing for CgPN (in addition to CdPN routing).<br><br>If selected, the I-CSCF performs ENUM query for the CgPN and routes to IMS for CgPN service if it is provisioned. If not selected, I-CSCF only performs CdPN routing.   |
| <b>Allowed Routes</b>      | Select one of the following options to specify allowed routes for the originating host. <ul style="list-style-type: none"><li>• IMS</li><li>• PSTN</li><li>• Transit-Sip</li></ul> One or more selections are allowed.<br>Transit-Sip means SIP termination outside the IMS domains of the operator. If no selection is made, checking for Allowed Route does not occur. |

For more information on the parameters, see the topic **RTCF Orig Host List Table** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

**6** Click **OK**.

**Result:** The Origination Host List table attributes are provisioned successfully.

END OF STEPS

# Wildcards in digit strings

## Introduction

Dialed digits are matched against the value that is specified in **String To Match**. This parameter can be specified based on a full digit string or a digit string that includes wildcards.

## Wildcards

The following wildcards for digit matching are supported:

| Wildcard | Description  |
|----------|--|
| P        | The digits represented by <i>P</i> in the match string can be either 0 or 1.<br>For example, the string P5088623000 will match either 05088623000 or 15088623000.  |
| N        | The digits represented by an <i>N</i> in the match string can be any number between 2 and 9.<br>For example, the string 508NN2N000 will match 5088623000, 5087724000, or any number that begins with 508, followed by two digits that can be any number between 2 and 9, followed by the number 2, followed by a single digit between 2 and 9 and ending with 000.   |
| X, Y, Z  | The digits represented by <i>X</i> , <i>Y</i> or <i>Z</i> in the match string can be any digit. For example, the matching string 508862XX00 will match any digit string that begins with 508862 followed by any two digits and ending with 00, such as 5088623000 or 5088629900.<br>These wildcards are interchangeable; however, X is generally preferred unless various parts of a number are specified. For example, the string XXXYYY1234 can be specified to indicate that the first three digits can be any value, the next three digits can be any value and the remaining digits must be 1234.<br>This is useful for translation purposes. For example, if you use the match string XXXYYY1234 and the translation string YYY&, the first three digits (XXX) are stripped from the digit string. |
| &        | The ampersand (&) specifies that all remaining digits can have any value. For example, the match string 508& will match any digit string that begins with 508 such as 5088623000, 5087783000, or 5081234.<br>Generally one should always place the & at the end of the match string to indicate that all remaining digits can be of any value. However, match strings that include only one character following an &, as in 508&#, are supported. This enables the possibility to strip a terminating digit or character.  |

Digit tables can be created with more than one attribute entry. The most specific digit string match is selected.

## Examples of digit matching

Digit matching examples are:

| Digit table<br>match string | Number to be<br>matched | Matching digit<br>string | Explanation  |
|-----------------------------|-------------------------|--------------------------|--|
| 5088623200                  | 5088623200              | 5088623200               | An exact match   |
| 5088623000                  | 5087783000              | 508XXX3000               | No exact match, but the first three digits are 508, the next three can be any value and the last three digits are 3000 |
| 508862&                     | 5088622400              | 508862&                  | No exact or more specific match, but the first six digits are 508862 and the remaining digits can be any value         |
| 508XXX3000                  | 5083859999              | 508&                     | No exact or more specific match, but the first three digits are 508 and the remaining digits can be any value          |
| 508&                        | 5088623000              | 5088623000               | An exact match   |

## Examples of digit translation

Digit string translation examples are:

| Number to be<br>matched | Match string | Translation string | Description   | Result        |
|-------------------------|--------------|--------------------|---|---------------|
| 6032253066              | 6032253066   | 1&                 | Insert 1 before the number                                | 16032253066   |
| 6032253066              | 603&         | 011603&            | Replace the digits to the left of the & (603) with 011603 | 0116032253066 |
| 6032253066              | 603&         | &                  | Remove the digits to the left of the & (603)              | 2253066       |
| 6032253066              | 603&         | 508&               | Replace the digits to the left of the & (603) with 508    | 5082253066    |
| 92253066                | 9&           | 603&               | Replace the digit to the left of the & (9) with 603       | 6032253066    |

| Number to be matched | Match string | Translation string | Description   | Result      |
|----------------------|--------------|--------------------|---|-------------|
| 6032253066           | 6032253066   | 6035551212         | Replace the digits in the match string with the digits in the translation string  | 6035551212  |
| 6032253066           | 603&         | &11                | Remove the digits to the left of the & (603) and append 11 to the number  | 225306611   |
| 8005551212           | 800555&      | &                  | Remove all digits to the left of the & (800555)   | 1212        |
| 8002221212           | 800XX&       | &                  | Remove all digits to the left of the & (80022)  | 21212       |
| 5085551212           | 508XXX&      | &603XXX            | Remove all digits to the left of the & (508555) and then append 603 and the original digits represented by XXX (555) to the end of the number | 1212603555  |
| 15553030             | X555YYYY     | YYYY555X           | Move the first digit (1) to the end of the number and move the last four digits (3030) to the beginning of the number                         | 30305551    |
| 15088623000          | YYYYZZZ&     | XZZZYYY&           | Transpose the digits represented by YYY (508) and those represented by ZZZ (862)  | 18625083000 |

| Number to be matched | Match string | Translation string | Description                      | Result  |
|----------------------|--------------|--------------------|----------------------------------|---------|
| 6169991#             | &#           | &                  | Remove the terminating character | 6169991 |

# To change the operational state of a host providing IMS Service

## Purpose

Use this procedure to change the operational state of a redundant set of hosts that provide IMS Service.

## Procedure

Perform the following steps:

1 In the MI tree view, expand the view to display the desired LCP and sublistings.

2 Double-click on **Services members**, and point at the desired IMS unit.

3 Right-click and a menu appears. Select and click **State Control**.

4

| If...  | Then...                                   |
|--|---|
| The IMS Server should be moved from the <i>OOS</i> Service state to the <i>IS</i> Service state, | Select <b>Switchover</b> .                |
| The SIPia port should gracefully be moved the <i>OOS</i> Service state,                          | Select <b>Force OOS</b> .                 |
| The SIPia port should directly be changed to the <i>OOS</i> Service state,                       | Select <b>Unconditionally Force OOS</b> . |

**Important!** When the IMS Server receives the response of OOS, then all associated SIPia ports service states change to OOS. Components associated with these SIPia ports de-register all of the UEs (for S-CSCF only) and release all of the resources associated with the users and their calls.

The following table shows the impact of changing states of a *P-CSCF* SIPia port:

| Current Service State | Move to State | Application Actions  |
|-----------------------|---------------|--|
| IS                    | SHUTDOWN      | <ul style="list-style-type: none"> <li>• No Action on existing call</li> <li>• Reject any new registration for the new user or user without active call involved</li> <li>• Do not block standalone request</li> <li>• Allow re-registration for the user with call involved</li> <li>• When all calls using this P-CSCF port are terminated, move SIPia port to <b>OOS</b></li> </ul> |
| IS                    | OOS           | <ul style="list-style-type: none"> <li>• Interrupt existing call</li> <li>• Interrupt the proxy subscription ICRs</li> <li>• Block standalone request</li> <li>• Reject any new registration</li> <li>• Delete the registry</li> <li>• If P-CSCF did SUBSCRIBE, cancel the SUBSCRIBE</li> <li>• When all the registries are deleted, move SIPia port to <b>OOS</b></li> </ul>          |
| SHUTDOWN              | IS            | <ul style="list-style-type: none"> <li>• Stop monitoring the existing call</li> <li>• Allow new session to be accepted</li> <li>• Signal to IMS manager for completion of <b>IS</b></li> </ul>   |
| OOS                   | IS            | <ul style="list-style-type: none"> <li>• If returning to <b>IS</b> before OOS completed, then application will stop the <b>OOS</b> action, but recovery of completed actions may not be possible</li> </ul>  |

The following table shows the impact of changing states of a *I-CSCF* SIPia port:

| Current Service State | Move to State | Application Actions  |
|-----------------------|---------------|--|
| IS                    | SHUTDOWN      | <ul style="list-style-type: none"> <li>• No action on existing call</li> <li>• Reject new call setup; however, REGISTER is allowed</li> <li>• When existing call is terminated, move SIPia port to <b>OOS</b></li> </ul> |

| Current Service State | Move to State | Application Actions   |
|-----------------------|---------------|---|
| IS                    | OOS           | <ul style="list-style-type: none"> <li>Reject any new registration</li> <li>When call is terminated, move SIPia port to <b>OOS</b></li> </ul>   |
| SHUTDOWN              | IS            | <ul style="list-style-type: none"> <li>Stop monitoring the existing call</li> <li>Accept new requests</li> <li>Signal back to SIPia port manager for <b>IS</b> completion</li> </ul>            |
| OOS                   | IS            | <ul style="list-style-type: none"> <li>If returning to <b>IS</b> before <b>OOS</b> completed, <b>OOS</b> action will be stopped; however, it may not fully recover completed actions</li> </ul> |

The following table shows the impact of changing states of a S-CSCF SIPia port:

| Current Service State | Move to State | Application Actions  |
|-----------------------|---------------|--|
| IS                    | SHUTDOWN      | <ul style="list-style-type: none"> <li>De-register the subscriber when there is no existing call</li> <li>When existing call is terminated, de-register the subscriber</li> <li>Subscriber de-registration results in registry deletion</li> <li>Reject any new registration and new call setup</li> <li>Reject re-registration for the UE when it has no existing calls</li> <li>When all PUIDs of one PRIVID are de-registered, send final NOTIFY to UE and P-CSCF to terminate subscription</li> <li>Move SIPia port to <b>OOS</b></li> </ul> |

| Current Service State | Move to State | Application Actions  |
|-----------------------|---------------|--|
| IS                    | OOS           | <ul style="list-style-type: none"> <li>De-register the subscriber when no call active</li> <li>Interrupt existing call, and at termination, de-register subscriber</li> <li>After subscriber de-registration, delete registry</li> <li>Reject any new registration and new call setup</li> <li>Reject re-registration for the UE if no existing call</li> <li>When all PUIDs are de-registered, send final NOTIFY to UE and P-CSCF to terminate the subscription</li> <li>Move SIPia port to <b>OOS</b></li> </ul> |
| SHUTDOWN              | IS            | <ul style="list-style-type: none"> <li>Tell SIPia port status to accept new requests</li> <li>Stop de-registration</li> </ul>  |
| OOS                   | IS            | <ul style="list-style-type: none"> <li>If <b>OOS</b> not completed, stop the process; however, completed parts may not be recovered</li> </ul>   |

The following table shows the impact of changing states of a *BGCF* SIPia port:

| Current Service State | Move to State | Application Actions  |
|-----------------------|---------------|--|
| IS                    | OOS           | <ul style="list-style-type: none"> <li>The SIPia stack no longer sends calls to the BGCF</li> </ul>                    |
| IS                    | SHUTDOWN      | <ul style="list-style-type: none"> <li>Notification is sent to the SIPia stack that the BGCF port is locked</li> </ul> |
| OOS                   | IS            | <ul style="list-style-type: none"> <li>New calls will be accepted</li> </ul>   |
| SHUTDOWN              | OOS           | <ul style="list-style-type: none"> <li>The SIPia stack will no longer send calls to the BGCF</li> </ul>                |
| SHUTDOWN              | IS            | <ul style="list-style-type: none"> <li>New calls will be accepted</li> </ul>   |

The following table shows the impact of changing states of a *UMRF* SIPia port:

| Current Service State | Move to State | Application Actions   |
|-----------------------|---------------|---|
| IS                    | OOS           | <ul style="list-style-type: none"> <li>The SIPia stack no longer sends calls to the UMRF</li> </ul> |

| Current Service State | Move to State | Application Actions  |
|-----------------------|---------------|--|
| IS                    | SHUTDOWN      | <ul style="list-style-type: none"> <li>Notification is sent to the SIPia stack that the UMRF port is locked</li> </ul> |
| OOS                   | IS            | <ul style="list-style-type: none"> <li>New calls will be accepted</li> </ul>   |
| SHUTDOWN              | OOS           | <ul style="list-style-type: none"> <li>The SIPia stack will no longer send calls to the UMRF</li> </ul>                |
| SHUTDOWN              | IS            | <ul style="list-style-type: none"> <li>New calls will be accepted</li> </ul>   |

**5 Select between Force OOS and Unconditional Force OOS.**

**Important!** When a host providing the IMS Service receives the response of **OOS**, then all associated SIPia ports service states change to **OOS**. Components associated with these SIPia ports de-register all of the UEs (for S-CSCF only) and release all of the resources associated with the users and their calls.

Those resources include:

- Private ID entries,
- Registries including the linkage to other resources,
- Implicit Registration Set,
- Service Profile (for S-CSCF only),
- Dialog,
- Call, and
- Inherited Calls.

The following table shows the impact of changing states:

| Component | Current Service State | Move to State | Application Actions  |
|-----------|-----------------------|---------------|--|
| P-CSCF    | IS                    | SHUT-DOWN     | <ul style="list-style-type: none"> <li>• No Action on existing call</li> <li>• Reject any new registration for the new user or user without active call involved</li> <li>• Do not block standalone request</li> <li>• Allow re-registration for the user with call involved</li> <li>• When all calls using this P-CSCF port are terminated, move SIPia port to <b>OOS</b></li> </ul> |
| P-CSCF    | IS                    | OOS           | <ul style="list-style-type: none"> <li>• Interrupt existing call</li> <li>• Interrupt the proxy subscription ICRs</li> <li>• Block standalone request</li> <li>• Reject any new registration</li> <li>• Delete the registry</li> <li>• If P-CSCF did SUBSCRIBE, cancel the SUBSCRIBE</li> <li>• When all the registries are deleted, move SIPia port to <b>OOS</b></li> </ul>          |
| P-CSCF    | SHUT-DOWN             | IS            | <ul style="list-style-type: none"> <li>• Stop monitoring the existing call</li> <li>• Allow new session to be accepted</li> <li>• Signal to IMS manager for completion of <b>IS</b></li> </ul>   |
| P-CSCF    | OOS                   | IS            | <ul style="list-style-type: none"> <li>• If returning to <b>IS</b> before OOS completed, then application will stop the <b>OOS</b> action, but recovery of completed actions may not be possible</li> </ul>  |
| I-CSCF    | IS                    | SHUT-DOWN     | <ul style="list-style-type: none"> <li>• No action on existing call</li> <li>• Reject new call setup; however, REGISTER is allowed</li> <li>• When existing call is terminated, move SIPia port to <b>OOS</b></li> </ul>   |
| I-CSCF    | IS                    | OOS           | <ul style="list-style-type: none"> <li>• Interrupt the existing call</li> <li>• Reject any new registration</li> <li>• When call is terminated, move SIPia port to <b>OOS</b></li> </ul>   |

| Component | Current Service State | Move to State | Application Actions  |
|-----------|-----------------------|---------------|--|
| I-CSCF    | SHUT-DOWN             | IS            | <ul style="list-style-type: none"> <li>Stop monitoring the existing call</li> <li>Accept new requests</li> <li>Signal back to SIPia port manager for <b>IS</b> completion</li> </ul>   |
| I-CSCF    | OOS                   | IS            | <ul style="list-style-type: none"> <li>If returning to <b>IS</b> before <b>OOS</b> completed, <b>OOS</b> action will be stopped; however, it may not fully recover completed actions</li> </ul>  |
| S-CSCF    | IS                    | SHUT-DOWN     | <ul style="list-style-type: none"> <li>De-register the subscriber when there is no existing call</li> <li>When existing call is terminated, de-register the subscriber</li> <li>Subscriber de-registration results in registry deletion</li> <li>Reject any new registration and new call setup</li> <li>Reject re-registration for the UE when it has no existing calls</li> <li>When all PUIDs of one PRIVID are de-registered, send final NOTIFY to UE and P-CSCF to terminate subscription</li> <li>Move SIPia port to <b>OOS</b></li> </ul> |
| S-CSCF    | IS                    | OOS           | <ul style="list-style-type: none"> <li>De-register the subscriber when no call active</li> <li>Interrupt existing call, and at termination, de-register subscriber</li> <li>After subscriber de-registration, delete registry</li> <li>Reject any new registration and new call setup</li> <li>Reject re-registration for the UE if no existing call</li> <li>When all PUIDs are de-registered, send final NOTIFY to UE and P-CSCF to terminate the subscription</li> <li>Move SIPia port to <b>OOS</b></li> </ul>                               |
| S-CSCF    | SHUT-DOWN             | IS            | <ul style="list-style-type: none"> <li>Tell SIPia port status to accept new requests</li> <li>Stop de-registration</li> </ul>  |

| Component | Current Service State | Move to State | Application Actions  |
|-----------|-----------------------|---------------|--|
| S-CSCF    | OOS                   | IS            | <ul style="list-style-type: none"> <li>If <b>OOS</b> not completed, stop the process; however, completed parts may not be recovered</li> </ul> |
| BGCF      | UNLOCKED              | LOCKED        | <ul style="list-style-type: none"> <li>The SIPia stack no longer sends calls to the BGCF</li> </ul>  |
| BGCF      | UNLOCKED              | SHUT-DOWN     | <ul style="list-style-type: none"> <li>Notification is sent to the SIPia stack that the BGCF port is locked</li> </ul>                         |
| BGCF      | LOCKED                | UNLOCKED      | <ul style="list-style-type: none"> <li>Service state changes from <b>OOS</b> to <b>IS</b></li> </ul>   |
| BGCF      | SHUTTING DOWN         | LOCKED        | <ul style="list-style-type: none"> <li>The SIPia stack will no longer send calls to the BGCF</li> <li>Service state is <b>OOS</b></li> </ul>   |
| BGCF      | SHUTTING DOWN         | UNLOCKED      | <ul style="list-style-type: none"> <li>New calls will be accepted</li> <li>Service state is <b>IS</b></li> </ul>                               |

6 Click **Close**.

7 Pointing at the impacted IMS unit, right-click and a menu appears. Select **Summarize Properties**.

8 Observe the **opState** entry in the **3gpp-State** area of the screen.

9 Click **Close**.

END OF STEPS

# To change the operational or administrative state of a SIPia port

## Purpose

Use this procedure to change the operational or administrative state of a SIPia port.

*Note:* On the FS GUI the hosts providing the IMS, 5420 CTS Services are referred to as the Next-Generation SIP Servers (NGSS).

## Procedure

Perform the following steps:

1 In the FS GUI toolbar, click **System View**.

2 Click “+” next to **Services** and the following subjects appear.

- **IMS**
- **5420 CTS**

3 If needed, click **Refresh States**.

4

| If   | Then  |
|--|---|
| you want to change the IMS SIPia port      | Click “+” next to <b>IMS</b> and <b>IMS Service</b> appears.<br>Click “+” next to <b>IMS Service</b> and the SIPia port icon appears.               |
| you want to change the 5420 CTS SIPia port | Click “+” next to <b>5420 CTS</b> and <b>5420 CTS Service</b> appears<br>Click “+” next to <b>5420 CTS Service</b> and the SIPia port icon appears. |

5 Double-click **SIPia Port** to open the SIPia port window.

6 Observe Port Name, Port Type, Port number, Administrative State, Operational State, and Service State.

- 7 Select the Port Name for which the administrative state should be changed.
- 8 **Important!** Selecting the **Lock** option for the SIPia port, the RF connection to the CCF will be torn down immediately.  
In this case the ACR message generation for any active call is rigorously interrupted.  
To shut down the ACR message generation gracefully, the *shut down* operation must be used.

Right-click on the selected port name.

| If...  | Then...                            |
|--|------------------------------------|
| The SIPia port should be moved from the <i>OOS</i> Service state to the <i>IS</i> Service state, | Select the <b>Unlock</b> option.   |
| The SIPia port should gracefully be moved to the <i>OOS</i> Service state,                       | Select the <b>Shutdown</b> option. |
| The SIPia port should directly be changed to the <i>OOS</i> Service state,                       | Select the <b>Lock</b> option.     |

**Important!** When the SIPia port state is changed from **Unlock** state, the IMS or 5420 CTS manager eventually sends the response **OOS**, and then the SIPia port service state also becomes **OOS**. Components associated with this SIPia port deregister the user (for S-CSCF only) and release the resources associated with the user and the call.

- 9 If needed, click **Refresh States**.
- 10 Click **Close**.

END OF STEPS

# To view the operational state of a host providing IMS Service

## Purpose

Use this procedure to view the operational state of a redundant set of hosts that provide IMS Service.

## Procedure

Perform the following steps:

- 1 In the MI tree view, expand the view to display the desired LCP and sublistings.
- 2 Double-click on **Services** and point at the desired IMS unit.
- 3 Pointing at the desired IMS unit, right-click and a menu appears. Select **Summarize Properties**.
- 4 Observe the **opState** entry in the **3gpp-State** area of the screen.
- 5 Click the **Close** button.

END OF STEPS

## To view the administrative state of a SIPia port

### Purpose

Use this procedure to view the administrative state of a SIPia port.

### Procedure

Perform the following steps:

- 
- 1 On the toolbar of the FS GUI, click **System View**. In the **System View** window that appears, expand the **Services** folder.
- 

- 2 Select the required service, for example **IMS**, and expand the folder..

Result: the menu tree of the service group is visible

- 
- 3 Expand the service group.

Result: the menu tree of the service group is visible

- 
- 4 Click the **Sipia Port** to open the window.

Result: in the right window the **Administrative State** is visible

- 
- 5 Observe **Port Name**, **Port Type**, **Administrative State**, **Operational State**, and **Service State**.
- 

- 6 Click the **Close** button.

END OF STEPS

---

# Verifying operational functionality using the **ims\_cli** command

## Description

The **ims\_cli** command provides the following functionality:

- Dump virtual group data

The **ims\_cli** command is used to dump data of virtual group

- Call trace

Based on the criteria of SIP message content including To, From, R-URI, P-Asserted-ID to trace SIP messages received or sent from/to the ISC components, including P/I/S-CSCF, BGCF, E-CSCF, IBCF, IMS-GWF and iAGCF. If the initial SIP message of a call matches the criteria, the call will be traced. The trace output is in protocolmonitor.log.

- IMS registry query

Query IMS user's registry information by using the Public ID or Private ID and get the information from protocolmonitor.log.

- IMS Security Gateway Control Function

Dump the SGCF number of IPsec SA rules in use and provide it in protocolmonitor.log.

- IMS UE address query

The IMS UE address query is the IMS UE IP address:port, and IP address of the SBC serving the IMS UE (if available). The output is in protocolmonitor.log or the screen based on setting.

- Dump IMS UE registration

Use the **ims\_cli** command to dump the total number of registries within the S-CSCF, including both registered and unregistered user cases for an UE.

- IMS UE de-registration

Use the **ims\_cli** command is to de-register an UE.

- IMS call status query

Use the **im\_cli** command to query the status of a call using the Private ID or Public ID.

- IMS call release

Use the command to release active calls using the Private ID or Public ID along with the call ID.

- P-CSCF switch-back

When the original P-CSCF is recovered to in-service state, use the **im\_cli** command to inform the IBC to use the original P-CSCF.

- S-CSCF switch-back

Use the **im\_cli** command to inform the I-CSCF to use the original S-CSCF.

- 3GPP IBC switch-back

When the primary IBC is recovered to in-service state, use the **im\_cli** command to inform the secondary IBC to reject new registration with a rejection percentage to avoid registration storm.

**Note:** The **ims\_cli** command is applicable only on the Configuration server of the 5400 LCP.

## Dump virtual group data

### Tasks

The **ims\_cli** allows the query of the following per virtual group current concurrent session and bandwidth information:

- Incoming Current Concurrent Session
- Outgoing Current Concurrent Session
- Incoming Session Current Concurrent Bandwidth
- Outgoing Session Current Concurrent Bandwidth

### Synopsis

```
ims_cli -a <action> -t <type> -v <virtual group ID> [-v1 <virtual group count>] {Address}
```

The {Address} format is as follows:

|                           |   |
|---------------------------|---|
| Node                      | <b>-n ims</b>                           |
| Fixed Internal Service IP | <b>-i &lt;IP address in .format&gt;</b> |

### Parameters

- a The option is used to get virtual group data.
- t The option indicates the type of virtual group information query.
- v The option indicates the virtual group number. The maximum number is 1024.
- v1 The option indicates how many virtual groups need to be dumped
- i The option is used as existing.
- n The option is used as existing.

### Examples

```
ims_cli -a get -t vg -v 1000 -v1 2 -n ims
ims_cli -a get -t vg -v 0 -i[internal fix IP]
```

**Call trace****Synopsis**

```
ims_cli -a <action> -t sip_mon -v <0-29> -v1 <0-6> -p <parameter> -s
<string> -p1 -substring -s <string> -T <interval> {Address}
```

**Parameters**

**-a** The <action> indicates which action should be taken.

- clr: Initialize the Sip Monitor
- alw: Enable the Sip Monitor
- inh: Disable the Sip Monitor
- get: Get Sip Monitor status
- set: Set the parameter to be traced

**-t sip\_mon** This options indicates that it is call trace for ims\_cli.

**-p** The options are:

- toheader: SIP To Header.
- fromheader: SIP From Header.
- PAIheader: SIP P\_Asserted\_Identity
- requiri: SIP Request URI to be monitored.
- mid: Getaway Identifier
- telnum: Telephone number

**-s** It is the content of option “-p”.

**-v** This option indicates the component to be traced.

The value for the components are as follows:

| Number | Component          |
|--------|--------------------|
| 0      | for all components |
| 1      | ICSCF              |
| 2      | PCSCF              |
| 3      | SCSCF              |
| 4      | BGCF               |
| 10     | ECSCF              |
| 19     | IBCF               |
| 24     | GWF                |
| 26     | iAGCF              |
| 28     | CANM               |
| 29     | H248 Proxy         |

- v1      This option indicates the trace ID. The range is from 0-6.
    - 0 indicates all traces (that is 1-6).
  - T      This option should not be greater than 2880 minutes.
  - r      The maximum size is 50.
- {Address}
- -n ims
  - -i: internal fixed IP;
- p telnum      This option indicates the criteria is set for one telephone number.  
The telephone number length must be in the range of 4–15.
- p mid      This option indicates MID for H248 proxy or Gateway ID for iAGCF.  
The MID length cannot exceed 256.
- p1 substring      This option indicates Substring for H248 Proxy or Message Type for iAGCF.  
The Substring length cannot exceed 256.  
The valid values for message type of iAGCF are as follows:
- 1 – Trace Call Messages
  - 2 – Trace ServiceChange messages
  - 3 – Trace subscriber Audit and Arming messages
  - 4 – Trace ALL messages
- Trace ID 0 is allowed when action is not SET.

### Examples

```
ims_cli -a clr -t sip_mon -v1 0 -i 10.122.154.2
ims_cli -a set -t sip_mon -p requiri -v 0 -v1 1 -r "abcd:" -T 60 -s "sip:
+17339900001@lucent.com" -i 10.122.154.2
ims_cli -a alw -t sip_mon -v1 1 -i 10.122.154.2
```

H248 proxy setting call trace by command line

```
ims_cli -a set -t sip_mon -v 29 -v1 <0x000001-0x000006> -p mid -s xxxx -
p1 substring -s xxxx -n ims
```

P-CSCF setting call trace by COM

```
ims_cli -a set -t sip_mon -v 2 -v1 <0x000001-0x000006> -p fromheader -s
xxxx -o com -n ims
```

iAGCF setting call trace by command line

```
ims_cli -a set -t sip_mon -v 26 -v1 <0x000001-0x000006> -p mid -s xxxx -
p1 substring -s 1 -n ims
```

Telephone number call trace setting (left part) by command line

```
ims_cli -a set -t sip_mon -v 0 -v1 2 -p telnum -s 153686 -p1 substring -
s left -n ims
```

**IMS registry****Synopsis**

```
ims_cli -a <action> -t <type> -p <parameter> -s <string> [-v <component
type 2-3>] {Address}
```

**Parameters**

-a The <action> indicates which action should be taken.

- get: Get Registry info.

-t reg This option indicates that it is IMS Registry Query for ims\_cli.

-p The options are:

- privid: Private URI.
- puid: Public URI.

**Note:** The subscriber service profile is included in the output only when the PUID is applied in the registration query. This note is applicable to S-CSCF only.

-s {Private ID} or {PUID URI}

-v This option indicates the component type in integer format.

The options are:

- 2: P-CSCF
- 3: S-CSCF . The default value is 3.

{Address}

- -n ims
- -i: internal fixed IP;

**Example**

```
ims_cli -a get -t reg -p privid -s
"privateid01@qa001.qd.lucentlab.com" -v 2 -n ims
ims_cli -a get -t reg -p puid -s "sip:
+16309792001@qa001.qd.lucentlab.com" -v 2 -n ims
```

For Emergency Registration, this command shows all existing contacts (include emergency contact if it is registered) in the output. The count of puid and privid are not impacted by emergency contact if a set of puid and privid has both contacts registered, puid 1 and privid 1 are only counted.

**IMS security gateway control function****Synopsis**

```
ims_cli -a <action> -t <type> -p <parameter> [-s <string>] {Address}
```

**Parameters**

-a The <action> indicates which action should be taken.

- get: Get the usage of IPSec Rules.

-t sgcf This options indicates that it is IMS Security Gateway Control Function for ims\_cli.

-p The options are:

- cnt: count.

-s za: za interface

{Address}

- -n ims
- -i: internal fixed IP;

#### Example

```
ims_cli -a get -t sgcf -p cnt -s za -i 10.122.154.2
```

## IMS UE address

#### Synopsis

```
ims_cli -a <action> -t <type> -p <parameter> -s <string> -o screen  
{Address}
```

#### Parameters

-a The <action> indicates which action should be taken.

- get: Get UE address and SBC address (if available).

-t ueaddr This options indicates that it is IMS UE address query for ims\_cli.

-p The options are:

- privid: private URI

-s {Private ID}

-o screen The output is in protocolmonitor.log and the screen.

{Address}

- -n ims
- -i: internal fixed IP;

#### Examples

```
ims_cli -a get -t ueaddr -p privid -s
```

"privateid01@qa001.qd.lucentlab.com" -o screen -i 10.122.154.2 The output is in protocolmonitor.log and the screen.

```
ims_cli -a get -t ueaddr -p privid -s
```

"privateid01@qa001.qd.lucentlab.com" -i 10.122.154.2 The output is in protocolmonitor.log

---

## Dump IMS UE registration

### Synopsis

```
ims_cli -a <action> -t reg -p <parameter>[-v <component type 2 - 3>] {Address}
```

### Description

The command mentioned above is used dump the total number of registries within the S-CSCF or P-CSCF, including both registered and unregistered user cases for an UE.

### Parameters

-a      The <action> indicates which action should be taken.

- get: Get Registry info.

-t reg     This option indicates that it is IMS registry query for ims\_cli.

-p      The option is:

- cnt:count

-v      This option indicates the component type in integer format.

The options are:

- 2: P-CSCF
- 3: S-CSCF . The default value is 3.

{Address}

- -n ims
- -i: internal fixed IP;

### Example

```
ims_cli -a get -t reg -p cnt -v 2 -n ims
```

## IMS UE de-registration

### Synopsis

```
ims_cli -a <action> -t <type> -p <parameter> -s {Private ID} [-p1 puid - s {PUID URI}] [-o screen] [-v <component type 2 - 3>] {Address}
```

### Description

The command mentioned above is used to de-register an UE. For de-registration, all the associated active calls will be released, except the calls that are not involved or associated with the UE. The calls that are not involved or associated with the UE are the calls that are transferred or forwarded from the UE.

**Note:** An emergency call is not allowed to be released through de-registration.

**Note:** For AGCF/IPPBX user de-registration, only GW private ID of AGCF/IPPBX is allowed. If the command mentioned above is used for AGCF/IPPBX all users registered under the AGCF/IPPBX will be de-registered.

## Parameters

- a      The <action> indicates which action should be taken.
  - clr: This option is used to clear UE registration.
- t reg    This option indicates that it is IMS registry query for ims\_cli.
- p      The option is:
  - privid: private URI
- s      {Private ID}
- o screen    The output is produced in protocolmonitor.log and the screen.  
{Address}
  - -n ims
  - -i: internal fixed IP;
- v      This option indicates the component type in integer format.

The options are:

- 2: P-CSCF
- 3: S-CSCF . The default value is 3.

## Example

```
ims_cli -a clr -t reg -p privid -s  
"privateid01@qa001.qd.lucentlab.com" -v 2 -n ims
```

**Note :** Wildcard matching is not supported for de-registration. For instance, a distinct input PUID string matching the wildcard PUID is not supported to de-register users. For example, the PUID provisioned in HSS is with the wildcard, like: “tel:123456![0-9][0-9]!”, but de-registration with input PUID tel:12345678 is NOT supported to de-register users although it matches the provisioned wildcard PUID. Only the exact matched PUID string with the provisioned HSS can de-register the users, that is: **ims\_cli -a clr -t reg -p privid -s private\_id@example.com -p1 puid -s tel:123456![0-9][0-9]! -n ims**.

## IMS call query

### Synopsis

```
ims_cli -a <action> -t call -p privid -s {Private ID} [-v  
<component type 2 - 3>] {Address}  
  
ims_cli -a <action> -t call -p puid -s {PUID URI} [-v <component  
type 2 - 3>] {Address}
```

### Description

The command mentioned above is used to query the call status by using the Private ID or the Public ID.

A call is generally associated with a PUID. Its association with the PRID varies for different cases. The calls that are not linked to a PRID mainly include:

- Unregistered user's call (either unregistered origination or termination)
- AS originated call on behalf of UE
- AS terminated call
- AS forwarded call

For calls that are not linked to a PRID, the call status query using PRID will not display the call information.

### Parameters

- a      The <action> indicates which action should be taken.
  - get: This option is used to query UE call status.
- t call    This option indicates that it is IMS call query for ims\_cli.
- p      The option is:
  - privid: private URI
  - puid: public URI
- s      The applicable options are:
  - {Private ID}
  - {Public ID}
- v      This option indicates the component type in integer format.

The options are:

- 2: P-CSCF
- 3: S-CSCF . The default value is 3.

{Address}

- -n ims
- -i: internal fixed IP;

### Examples

```
ims_cli -a get -t call -p privid -s
"privateid01@qa001.qd.lucentlab.com" -v 2 -n ims

ims_cli -a get -t call -p puid -s "sip:
+16309792001@qa001.qd.lucentlab.com" -v 2 -n ims
```

**Note :** A distinct PUID string that matches the wildcard PUID is not supported to query a call. However, the wildcard PUID string can be used, for example tel:123456![0-9][0-9]!, but PUID tel:12345678 is not supported to query calls. The wildcard PUID string should be the one provisioned in the HSS.

For emergency registration, the output indicates if the contact used by the call is an emergency contact or not.

## IMS call release

### Synopsis

```
ims_cli -a clr -t call -p privid -s {Private ID} -p1 puid -s {PUID URI}
        [-p2 callid -s {Call ID}] [-T <timeinterval>] [-o screen] [-v
        <component type 2 - 3>] {Address}
ims_cli -a clr -t call -p puid -s {PUID URI} [-p1 callid -s {Call ID}] [-
        T <timeinterval>] [-o screen] [-v <component type 2 - 3>] {Address}
```

### Description

The command mentioned above is used to release active calls by using the Private ID or Public ID along with the call ID.

A call is generally associated with a PUID. Its association with the PRID varies for different cases. The calls that are not linked to a PRID mainly include:

- Unregistered user's call (either unregistered origination or termination)
- AS originated call on behalf of UE
- AS terminated call
- AS forwarded call

If the PRID is specified in the command, the calls linked to the indicated PRID will be released, while those not linked to this PRID will not get impacted.

For **-T** option, the time interval range is 30 - 600 (seconds). If **-T** option is specified, the **-o** option is suppressed.

### Parameters

- a      The <action> indicates which action should be taken.
  - clr: It means clear/release the call. Initialize the SIP monitor.
- t call    This option indicates that it is IMS call query for ims\_cli.
- p      The options are:
  - privid: private URI
  - puid: public URI
  - callid: call ID
- s      The options are:
  - {Private ID}
  - {Public ID}
  - {Call ID}
- o screen   The output is produced in protocolmonitor.log and the screen.
- v      This option indicates the component type in integer format.  
The options are:
  - 2: P-CSCF
  - 3: S-CSCF . The default value is 3.

{Address}

- -n ims
- -i: internal fixed IP;

**Examples**

```
ims_cli -a clr -t call -p privid -s
"privateid01@qa001.qd.lucentlab.com" -p1 puid -s "sip:
+16309792001@qa001.qd.lucentlab.com" -v 2 -n ims

ims_cli -a clr -t call -p puid -s "sip:
+16309792001@qa001.qd.lucentlab.com" -v 2 -n ims

ims_cli -a clr -t call -p puid -s "sip:
+16309792001@qa001.qd.lucentlab.com" -T 100 -v 2 -n ims

ims_cli -a clr -t call -p puid -s "sip:
+16309792001@qa001.qd.lucentlab.com" -o screen -v 2 -n ims

ims_cli -a clr -t call -p puid -s sip:public_
id01@g1112.ate.lucentlab.com -p1 callid -s LU-
1268032891131602@imsgroup0-001.g1112.ate.lucentlab.com -v 2 -i
10.76.154.1

ims_cli -a clr -t call -p privid -s private_
id01@g1112.ate.lucentlab.com -p1 puid -s sip:public_
id01@g1112.ate.lucentlab.com -p2 callid -s LU-
1268032891131602@imsgroup0-001.g1112.ate.lucentlab.com -v 2 -i
10.76.154.1
```

**BEPH manual Sync**

BEPH manual sync request is invoked in order to repair or recover FEPH flow data without having to duplex fail FEPHs (autonomous BEPH sync takes place on the occasion of FEPH duplex fail).

The format of the CLI command for the option of first wiping out the FEPH flow data (flow tables and IP flow tables) prior to starting BEPH sync is as follows:

```
ims_cli -a set -t bephsync -d clear -n feph
```

The format of the CLI command for the option of starting BEPH sync on top of existing FEPH flow data, akin to auditing that data's flow and IP flow policies and policy expiration, is as follows:

```
ims_cli -a set -t bephsync -n feph
```

## P-CSCF switch-back

### Description

When the original P-CSCF is recovered to in-service state, this **ims\_cli** command is used to inform the 3GPP IBC to use the original recovered P-CSCF. The 3GPP IBC checks the set or clear flag in this command when choosing the P-CSCF only on UE reregister. When clearing original service route, the original service route in binding is saved and reused for routing when the original service route is recovered. The switchback percentage allows the 3GPP IBC to move users to the recovered registered P-CSCF gradually. It must be set appropriately so as to avoid causing registration storm on the recovered P-CSCF.

### Synopsis

```
ims_cli -a set|get|clr -t rec -v pcscf -p <recovery percentage>  
{Address}
```

### Parameters

**-a** This parameter indicates the action that needs to be taken.

- **set:** This option is used to set the Recover flag.
- **get:** This option is used to get the Recover flag
- **clr:** This option is used to clear the Recover flag.

**-t rec** This parameter indicates that the function type is recovery.

**-v pcscf** This parameter indicates that this command is for P-CSCF pool recovery

**-p <recovery percentage>** This parameter is used to specify the recovery percentage. The <recovery percentage> indicates the recovery percentage which allows the 3GPP IBC to move users to initially registered P-CSCF gradually. The range is from 1 to 100, and the default value is 100. This parameter is mandatory.

**{Address}** The options are as follows:

- **-i [ip]:** This option is used to send the register request to IBC of one IMS service
- **-n ims:** This option is used to send the register request to IBC of all IMS services

## S-CSCF switch-back

### Description

When the original S-CSCF is recovered to in-service state, this **ims\_cli** command is used to inform the I-CSCF to use the original recovered S-CSCF. The I-CSCF checks the set or clear flag in this command when choosing the S-CSCF only on UE reregister.

### Synopsis

```
ims_cli -a set|get|clr -t rec -v scscf {Address}
```

**Parameters**

- a This parameter indicates the action that needs to be taken.
  - set: This option is used to set the Recover flag.
  - get: This option is used to get the Recover flag
  - clr: This option is used to clear the Recover flag.
- t rec This parameter indicates that the function type is recovery.
- v scscf This parameter indicates that this command is for S-CSCF pool recovery
- {Address} The options are as follows:
  - -i [ip]: This option is used to send the register request to I-CSCF of one IMS service
  - -n ims: This option is used to send the register request to I-CSCF of all IMS services

**3GPP IBC geo-redundancy switch-back****Synopsis**

```
ims_cli -a set|get|clr -t rec [-T <validity duration>] -p <rejection percentage> {Address}
```

**Description**

When the primary 3GPP IBC is recovered to in-service state, this **ims\_cli** command is used to inform the secondary IBC to reject new registration with a percentage to avoid registration storm. The 3GPP IBC GR switch-back is enabled only when geo-redundancy is enabled and the CLI command is set to the secondary IBC. The secondary IBC rejects initial REGISTER, re-REGISTER, and query REGISTER.

**Parameters**

- a The <action> indicates which action should be taken.
  - set: This option is used to set the Recover flag.
  - get: This option is used to get the Recover flag
  - clear: This option is used to clear the Recover flag.
- t rec This parameter indicates that the function type is recovery.
- T <validity duration> This parameter indicates the how long the flag is valid. The value range is from 10 to 4320 minutes, the default value is 30 minutes.
- p <rejection percentage> This parameter is used to specify the rejection percentage. The rejection percentage allows the IBC to reject the registration requests from the user gradually. The value range is from 1 to 100. This parameter is mandatory.

{Address} The options are as follows:

- -i [ip]: This option is used to send the register request to IBC of one IMS service
- -n ims: This option is used to send the register request to IBC of all IMS services

## SIP Link Manager Functions

A capability is provided for the operator to query current linkset, remove a linkset that is currently on the quarantine list and send manual heartbeat through the IMS CLI. The IMS CLI supports the Internal Quarantine List query control option as follows.

The following three SLM functions are added as part of the feature SIP heartbeat after failure to reach a network element:

- **for quarantine list query**

Inputs

- None
- Outputs - (Done in SLM callback);
- Whole quarantine list support output on screen.

Usage: **ims\_cli -a get -t sip\_hb [-o screen] {Address}**

Output: available linksets information and the output is in protocolmonitor.log and screen (if set -o screen).

- **for quarantine list deletion**

Inputs

- Destination Address (mandatory, could be FQDN, IPv4 or IPv6 without port)
- Transport (optional, could set to UDP/udp, TCP/tcp, TLS/tls, SCTP/sctp and default to all transport types if not specified)
- Port (Optional, default to all if not specified)

Outputs - (Done in SLM callback);

- if the deletion was a successful or failure action.
- support output on screen.

Usage:

```
ims_cli -a clr -t sip_hb -p addr -s {Destination} [-p1  
transport -s {Transport}] [-v {port}] [-o screen] {Address}  
{Transport}: tcp, udp, sctp, icmp
```

Output - A warning is provided and confirmation is required for the action invocation. The action execution result is in protocolmonitor.log and screen (if set -o screen). The output shall include if the deletion was a successful or failure action.

- **for a manual HB request**

---

### Inputs

- Destination Address (mandatory, could be FQDN, IPv4 or IPv6 without port)
- Transport (optional, could set to UDP/udp, TCP/tcp, TLS/tls, SCTP/sctp and default to all transport types if not specified)
- Port (Optional, default to all if not specified)

Outputs - (Done in SLM callback);

- Destination Address
- Port
- linkset status

### Usage:

```
ims_cli -a set -t sip_hb -p addr -s {Destination} [-p1  
transport -s {Transport}] [-v {port}] [-o screen] {Address}
```

{Transport}: tcp, udp, sctp, icmp

Output - The action execution result is in protocolmonitor.log and screen (if set –o screen). The output shall include if the manual heartbeat was a successful or failure action.

Service Addressing options:

Node: **-n ims**

Fixed Internal Service IP: **-i <ip address in .format>**

# To provision an External Domain Routing table

## Purpose

This procedure is used to provision an External Domain Routing table.

## Description

The External Domain Routing table is used for routing by the P-CSCF, I-CSCF, BGCF, S-CSCF, and internal IBCF.

During the S-CSCF ENUM query, when the query fails and the domain is not local, the domain needs to be resolved. In this case the external domain route table can be used.

We use the External Domain Routing table in P-CSCF for Roaming Registration.

When an Interconnection Border Control Function (IBCF) service component is provisioned, the association between the inter-network domains and the IBCF is established through the External Domain Routing table. This table contains domain-to-IBCF mapping information for call-processing, so outbound requests are routed to the appropriate IBCF (exit point). The IBCF (exit point) routes the request to the external network based on the Request-URI.

For IBCF, when the domain is not home domain or Local zone, then the external home domain table is checked to see if we have an entry for the external domain. When a matching entry is found and the next hop is provisioned, then the request is routed to the next hop. The next hop requires the DNS query to resolve the FQDN. When the external domain table has an entry but the next hop is not provisioned the default IBCF is used. When the external domain table is empty, then it is routed to the default IBCF. So, if more than one IBCF is required, then the external home domain table provisioning is required with next hop as ibcf.

## Before you begin

Observe the following:

1. When a table is created, a default **table number** is assigned by the system. Alcatel-Lucent recommends retaining the default value.
2. Only one External Domain Routing table can be created.

## Steps to provision an External Domain Routing table

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **IMS → IMS General Tables**.

**Result:** The **IMS General Tables** window is displayed.

- 2 In the left pane, expand the **External Domain Routing** folder.

**Result:** The External Domain Routing tables are listed under the folder in the left pane.

If the folder is empty, add an External Domain Routing table.

Perform the following steps in the **IMS General Tables** window to add, rename, or delete an External Domain Routing table :

| If you want to ...                       | then ...  |
|--|---|
| add an External Domain Routing table,    | <ol style="list-style-type: none"> <li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add External Domain Routing table</b> window is displayed.</li> <li>2. From the <b>Table Number</b> list, select the table number.</li> <li>3. In the <b>Table Name</b> box, type a descriptive table name.</li> <li>4. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| rename an External Domain Routing table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename External Domain Routing table</b> window is displayed.</li> <li>2. In the <b>Table Name</b> box, type a new table name.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>  |
| delete an External Domain Routing table, | <ol style="list-style-type: none"> <li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li> <li>2. Click <b>Yes</b> to confirm deletion</li> </ol> <p><b>Note:</b> Before you delete an External Domain Routing table, ensure that no table entries are in use.</p> <p><i>End of steps</i></p>  |

- 3 Double-click the table to open the list of profiles defined for the table.

Add the External Domain Routing table profiles to the newly created table. You can add, modify, or delete the attributes of existing profiles.

- 4 Perform the following steps at the **IMS General Tables** window to add, modify, or delete the External Domain Routing table attributes:

| If you want to ...                                  | then ...   |
|---|--|
| add the External Domain Routing table attributes,   | <ol style="list-style-type: none"> <li>Select <b>Attributes → Add Table Attributes.</b><br/><b>Result:</b> The <b>External Domain Routing</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p>  |
| modify an External Domain Routing table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes → Modify Table Attributes.</b><br/><b>Result:</b> The <b>External Domain Routing</b> window is displayed.</li> <li>Continue with <a href="#">Step 5</a> to provision the parameters.</li> </ol> <p><i>End of steps</i></p> |
| delete an External Domain Routing table attributes, | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes → Delete Table Attributes.</b></li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p>                        |

- 5 Provision the following parameters:

| Parameter                 | Provisioning  |
|---------------------------|---|
| <b>External Domain ID</b> | Select a unique ID for the External Domain Routing.                       |
| <b>External Domain</b>    | Type the home domains as specified on P-NAPTR Region.                     |
| <b>Next Hop</b>           | Type the domain name of the port that is to be used for routing messages. |

| Parameter                 | Provisioning   |
|---------------------------|--|
| <b>Network Identifier</b> | Type the value to be added in the P-Visited_Network-Id headers of the SIP messages for external domains. |

For more information on the parameters, see the topic **External Domain Routing** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379

- 
- 6 Click OK.

**Result:** The External Domain Routing table attributes are provisioned successfully.

END OF STEPS

---

# Service policy decision function

## Overview

### Purpose

This section contains common procedures for the Service Policy Decision Function (SPDF). Some of these procedures are stand-alone procedures while the remaining are referenced from various procedures as a part of the provisioning task flows.

### Contents

|   |        |
|---|--------|
| To provision a PDF profile                          | 10-104 |
| To provision a Diameter port                        | 10-108 |
| To lock, or unlock a Diameter port                  | 10-111 |
| To provision a variant                              | 10-114 |
| To provision a PPL component in a signaling variant | 10-116 |

# To provision a PDF profile

## Purpose

This procedure is used to provision a PDF port profile.

## Before you begin

### Points to remember:

- The PDF profile is assigned to a Diameter port to create a Policy Decision Functional Entity (PD-FE) service component.
- The IMS service provides a Diameter server capability that is used by service components that must function as a Diameter server. A Diameter server is provisioned by adding a Diameter port on an IMS service, which creates a particular service component on the IMS service. Each Diameter port must be associated with a profile where specific service component settings are defined.
- When you create a table, the system assigns a **table number**. The number can be changed, but Alcatel-Lucent recommends that you retain the default value.
- The PDF profile table supports a maximum of 64 profiles.
- A PDF profile must be assigned to a Diameter port on an IMS service to take affect.
- The PDF profile defines which Diameter interfaces are supported on the Diameter port.

## Steps to provision a PDF profile

Perform the following steps at the Provisioning GUI:

---

1 Select **IMS** → **IMS Components** → **PDF Tables**.

**Result:** The **PDF Tables** window is displayed.

In the left pane, expand the **PDF Profile** folder.

**Result:** The PDF Profiles are listed under the folder in the left pane.

If the folder is empty, add a PDF Profile table.

- 2 Perform the following steps in the **PDF Tables** window to add, rename, or delete a PDF Profile :

| If you want to ...    | then ...   |
|-----------------------|--|
| add a PDF Profile,    | <ol style="list-style-type: none"><li>1. Select <b>Tables</b> → <b>Add Table</b>.<br/><b>Result:</b> The <b>Add PDF Profile</b> window is displayed.</li><li>2. From the <b>Table Number</b> list, select the table number.</li><li>3. In the <b>Table Name</b> box, type a descriptive table name.</li><li>4. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p> |
| rename a PDF Profile, | <ol style="list-style-type: none"><li>1. Select the table, and then select <b>Tables</b> → <b>Rename table</b>.<br/><b>Result:</b> The <b>Rename PDF Profile</b> window is displayed.</li><li>2. In the <b>Table Name</b> box, type a new table name.</li><li>3. Click <b>OK</b>.</li></ol> <p><i>End of steps</i></p>   |
| delete a PDF Profile, | <ol style="list-style-type: none"><li>1. Select the table, and then select <b>Tables</b> → <b>Delete table</b>.</li><li>2. Click <b>Yes</b> to confirm deletion</li></ol> <p><i>End of steps.</i></p>  |

- 3 Double-click the newly created table. The table opens in the right pane. Perform the following steps at the **PDF Tables** window to add, modify, or delete the PDF Profile attributes:

| If you want to ...                 | then ...  |
|------------------------------------|---|
| add the PDF Profile attributes,    | <ol style="list-style-type: none"> <li>Select <b>Attributes</b> → <b>Add Table Attributes</b>.<br/><b>Result:</b> The <b>Policy Decision Function Profile Attributes</b> window is displayed.</li> <li>Provision the parameters in the <b>Policy Decision Function Profile Attributes</b> window and click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p>   |
| modify the PDF Profile attributes, | <ol style="list-style-type: none"> <li>In the right pane, select the profile that you want to modify.</li> <li>Select <b>Attributes</b> → <b>Modify Table Attributes</b>.<br/><b>Result:</b> The <b>Policy Decision Function Profile Attributes</b> window is displayed.</li> <li>Modify the parameters in the <b>Policy Decision Function Profile Attributes</b> window and click <b>OK</b>.</li> </ol> <p><i>End of steps</i></p> |
| delete a PDF Profile attributes,   | <ol style="list-style-type: none"> <li>In the right pane, select one or more profiles that you want to delete.<br/>To select multiple profiles, press <b>CTRL</b> and click the rows.</li> <li>Select <b>Attributes</b> → <b>Delete Table Attributes</b>.</li> <li>Click <b>Yes</b> to confirm deletion.</li> </ol> <p><i>End of steps</i></p>  |

The following figure illustrates the Policy Decision Function Profile Attributes window.

- Service Indication is only used in 3GPP2. The PD-FE uses Service Indication as a key while querying SPR
- When DSCP Profile ID is set to **default**, PD-FE connects to the BGW directly.

- 4 **Result:** The PDF Profile attributes are provisioned successfully.

For more information on the parameter description, see the topic, **PDF Profile Attributes** in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.

E N D   O F   S T E P S

# To provision a Diameter port

## Purpose

This procedure provides the steps to provision a Diameter port.

## Description

The IMS service provides a Diameter server capability that can be used by service components that must function as a Diameter server. A Diameter server is provisioned by adding a Diameter port on an IMS service, which creates a particular service component on the IMS service.

The Diameter port is used to create the following service components:

- Policy Decision Functional Entity (PD-FE)
- Vortex (Vrtx)

A Diameter port is similar in concept to a SIPia port: Each Diameter port has a unique Generic URI Label (GUL), a set of options that can be provisioned in various profiles, and an administrative state.

## Port profile

**Important!** Before you add a PD-FE Diameter port, you must create a PDF port profile. Each PD-FE Diameter port *must* be associated with a PDF port profile. If a PDF port profile does not exist, then the Diameter port cannot be created and an error message is displayed.

The type of configuration in the profile automatically defines which Diameter interface the Diameter server supports:

| Diameter port | Profile | Configuration        | Diameter interface | Diameter client   |
|---------------|---------|----------------------|--------------------|---|
| PD-FE         | PDF     | TISPAN<br>(Wireline) | Gq'                | Application Function: <ul style="list-style-type: none"><li>• P-CSCF</li><li>• IBCF</li></ul> |
|               |         |                      | Rw'                | Policy Enforcement Functional Entity: BGW   |
|               |         | 3GPP2<br>(Wireless)  | Tx                 | Application Function: P-CSCF  |
|               |         |                      | Ty                 | Access Gateway: PDSN  |

## Before you begin

Observe the following:

- An IMS service must exist.

To create an IMS service, refer to “[To provision an IMS Service association](#)” (p. 10-20).

- One IMS service can support up to 63 Diameter ports.

## Steps to provision a Diameter Port

Perform the following steps at the Provisioning GUI:

1 Click **System View**.

2 In the System View window, Expand the **Services** folder and then expand the **IMS** folder.

3 Expand the IMS Service folder of your choice and then select **Diam Port**.

**Result:** The right pane opens and displays the host provisioning data. After you click **Diam port**, the provisioning data and state information of the Diameter ports appears.

If no Diameter ports have been provisioned, no Diameter port will be displayed in the right pane.

| 4 | If you want to...       | then...  |
|---|-------------------------|--|
|   | add a Diameter port,    | <ul style="list-style-type: none"><li>• Right-click in the right pane and select <b>Add</b>.</li><li>• Specify the parameters in the Diameter Port Configuration window and click <b>OK</b>.</li><li>• Go to <a href="#">Step 5</a>.</li></ul>   |
|   | modify a Diameter port, | <ul style="list-style-type: none"><li>• Select the Diameter port that you want to modify, right-click, and click <b>Modify</b>.</li><li>• Modify the desired attributes and click <b>OK</b>.</li><li>• Go to <a href="#">Step 5</a>.</li></ul> <p><b>Note:</b><br/>All the attributes cannot be modified in this manner. To modify all the attributes delete the Diameter port and create a new Diameter port.</p> |

| If you want to...       | then...  |
|-------------------------|--|
| delete a Diameter port, | <ul style="list-style-type: none"> <li>Right-click the Diameter port and click <b>Lock</b>.</li> <li>Right-click the Diameter port and select <b>Delete</b>.</li> <li>Click <b>Yes</b> to confirm.</li> <li>Go to <a href="#">Step 5</a>.</li> </ul> |

- 5 When you have finished provisioning the Diameter ports, on the **File** menu, click **Exit**.

**Result:** The System View window closes.

END OF STEPS

### Provisioning data - PD-FE Diameter Port

Provision the parameters of the PD-FE Diameter port as follows:

| Parameter                   | Provisioning  |
|-----------------------------|---|
| <b>Port Type</b>            | Select <b>PDFE PORT</b> .   |
| <b>Port Name</b>            | Complete the GUL with the four-character port mnemonic (typically <i>stdn</i> ).<br><br>The port mnemonic specifies the PD-FE instance that is associated with a call that uses this Diameter port. Each IMS service supports up to 63 PD-FE instances, all with a different port name. |
| <b>Port number</b>          | 3868 (hard-coded, not provisionable)  |
| <b>Administrative State</b> | <i>Unlocked</i> (hard-coded, not used)  |
| <b>Port Profile</b>         | Select a PDF profile identifier.<br><br>The profile specifies which configuration the PD-FE that serves this Diameter port uses.  |
| <b>PDFE Distributor</b>     | Select whether the Diameter Port is a PD-FE Distributor or not.   |

# To lock, or unlock a Diameter port

## Purpose

This procedure provides the steps to manage administrative states of a Diameter port.

## Description

The Diameter port is used to create the following service components:

- Policy Decision Functional Entity (PD-FE)
- Vortex

A Diameter port is similar in concept to a SIPia port: Each Diameter port has a unique Generic URI Label (GUL) on one IMS service, a set of options that can be provisioned in various profiles, and an administrative state.

**Note:** DIAM port administrative state support is only for PD-FE. State management of Vortex policy engine is not supported.

## Administrative States

The operator can control and modify at any time the Administrative State of any Diameter port on any NGSS board in the system.

The Administrative States supported are:

- Lock
- Unlock

When the Diameter Administrative States is modified (from the Provisioning GUI), the NGSS (on the host) is immediately informed. The Diameter port Administrative State is displayed in the Provisioning GUI and MI GUI for each provisioned DIAM port in each NGSS. The Diameter Port supports the administration of state through Provisioning GUI. When right clicking the mouse button, a menu will pop up with the administration actions. When the administrative state is changed, the new state is saved in the database and sent to the IMS server with the existing Diam Port modify message.

## Call Processing

When placed in the Locked State, the Diameter Port rejects all received request messages, and tears down all existing sessions.

## Before you begin

Observe the following:

- An IMS service must exist.

To create an IMS service, refer to “[To provision an IMS Service association](#)” (p. 10-20).

- Full information about the provisioning parameters is provided in the *Alcatel-Lucent Control Platform 1000/1800/5400 Configuration Database Interface Specification and Object Descriptions Manual*, 275-900-379.
- One IMS service can support up to 63 Diameter ports.

## Procedure

Perform the following steps at the Provisioning GUI:

- 1 Click **System View**.
- 2 In the System View window, expand the **Services** folder and then expand the **IMS** folder.
- 3 Expand the IMS Service folder of your choice and then select **Diam Port**.

**Result:** The right pane opens and displays the host provisioning data. After you click **Diam port**, the provisioning data and state information of the Diameter ports appears.

| 4 | If you want to...       | then...   |
|---|-------------------------|---|
|   | lock a Diameter port,   | do the following: <ul style="list-style-type: none"> <li>• Select the Diameter port that you want to lock, and right-click, and click <b>Lock</b>.</li> </ul> |
|   | unlock a Diameter port, | do the following: <ul style="list-style-type: none"> <li>• Select the Diameter port that you want to unlock, right-click, and click <b>Unlock</b>.</li> </ul> |

**Note:** After you lock and then unlock the PDFE port, the connection between PCSCF and PDFE does not recover immediately and takes about an hour to do so. More actions are needed to recover it immediately. Click **DNS Look Up** on the Gq' diameter interface profile.

- 5 When you have finished managing the state of the Diameter ports, on the **File** menu, click **Exit**.

**Result:** The System View window closes.

END OF STEPS

# To provision a variant

## Purpose

This topic provides the steps to administer a signaling or data driven interworking variant.

## Before you begin

Observe the following information.

### Variant components

A variant consists of a set of programmable protocol language (PPL) components.

In some cases (such as H.248 GW variants), a new variant is still empty and you must import a file that contains the required PPL components. Refer to “[To provision a PPL component in a signaling variant](#)” (p. 10-116). Other variant types have default PPL components that are dynamically created when the variant is created.

### Constraint

When you modify a variant, you can merely change the name of the variant.

However, for each type of variant you can administer the set of PPL components. Refer to “[To provision a PPL component in a signaling variant](#)” (p. 10-116).

**Important!** Modifying PPL component settings can result in unexpected or unwanted results. Alcatel-Lucent technical support organizations provide changes when needed. Alcatel-Lucent strongly recommends that you do not modify PPL component settings unless you have consulted with Alcatel-Lucent.

### Deleting a variant

A variant can be deleted only when it is not being used.

## Steps to provision a variant

Perform the following steps at the Provisioning GUI:

- 
- 1 Select **System Admin → Variants**.

2 In the **Variants** window that appears, perform the following:

| If you want to    | Then   |
|-------------------|--|
| Add a variant,    | <ol style="list-style-type: none"><li>1. Select the variant type of your choice.</li><li>2. From the <b>Variant</b> menu, choose <b>Add Variant</b></li><li>3. In the new window that appears, enter a descriptive name and then click <b>OK</b></li><li>4. Proceed with the next step.</li></ol>  |
| Modify a variant, | <ol style="list-style-type: none"><li>1. Click the plus sign next to the variant type of your choice.</li><li>2. Select the variant that you want to modify</li><li>3. From the <b>Variant</b> menu, choose <b>Modify Variant</b>.</li><li>4. In the new window that appears, enter a new name and then click <b>OK</b></li><li>5. Proceed with the next step.</li></ol> |
| Delete a variant, | <ol style="list-style-type: none"><li>1. Click the plus sign next to the variant type of your choice</li><li>2. Select the variant that you want to delete</li><li>3. On the <b>Variant</b> menu, click <b>Delete Variant</b>.</li><li>4. In the dialog box that appears, click <b>Yes</b> to confirm</li><li>5. Proceed with the next step.</li></ol>                   |

3 Repeat Step 2 for each variant that you want to add, modify, or delete.

4 In Variants, click the **File** menu and then click **Exit**.

END OF STEPS

# To provision a PPL component in a signaling variant

## Purpose

This topic provides the steps to administer the programmable protocol language (PPL) components in a signaling variant.

## Before you begin

Observe the following information.

### Alcatel-Lucent technical support required

**Important!** Modifying PPL component settings can result in unexpected or unwanted results. Alcatel-Lucent technical support organizations provide changes when needed. Alcatel-Lucent strongly recommends that you do not modify PPL component settings unless you have consulted with Alcatel-Lucent.

### Prerequisite provisioning

You must have created the variant with PPL components in which you want to administer the PPL component. See topic *Add, modify, or delete a signaling variant*.

## Steps to provision a PPL component in a signaling variant

Perform the following steps at the Provisioning GUI:

- 1 Select **System Admin → Variants**.

**Result:** The **Variants** window appears.

- 2 In the **Variants** window that appears, expand the variant type folder of your choice and then double-click the variant of your choice.

**Result:** The PPL components are displayed in the pane on the right.

- 3 Do the following:

| If you want to       | Then  |
|----------------------|---|
| Add a PPL component, | <ol style="list-style-type: none"> <li>From the <b>PPL Component</b> menu, choose <b>Add Component</b></li> <li>In the <b>Advanced Parameter Provisioning</b> window that appears, define the new PPL component</li> <li>Proceed with the next step.</li> </ol> |

| If you want to          | Then  |
|-------------------------|---|
| Modify a PPL component, | <ol style="list-style-type: none"><li>1. Select the PPL component that you want to modify</li><li>2. From the <b>PPL Component</b> menu, choose <b>Modify Component</b></li><li>3. In the <b>Advanced Parameter Provisioning</b> window that appears, change the value as required</li><li>4. Proceed with the next step.</li></ol> |
| Delete a PPL component, | <ol style="list-style-type: none"><li>1. Select the PPL component that you want to delete</li><li>2. From the <b>PPL Component</b> menu, choose <b>Delete Component</b></li><li>3. In the dialog box that appears, click <b>Yes</b> to confirm</li><li>4. Proceed with the next step.</li></ol>                                     |

- 4 Repeat Step 3 for each PPL component that you want to add, modify, or delete.
- 5 In Variants, click the **File** menu and then click **Exit**.

END OF STEPS



# Part VI: Conformance and hazard statements

## Overview

### Purpose

This part of the documentation provides all the safety warnings, dangers and cautions that are used in this manual.

### Contents

|  |      |
|--|------|
| <a href="#">Chapter 11, Conformance statements</a> | 11-1 |
| <a href="#">Chapter 12, Hazard statements</a>      | 12-1 |



# 11 Conformance statements

## Overview

### Purpose

This chapter provides the product performance statements.

### Contents

|                              |      |
|------------------------------|------|
| 5400 LCP compliance summary  | 11-2 |
| Eco-environmental statements | 11-3 |

---

# 5400 LCP compliance summary

## Purpose

This topic gives a summary of compliance of the 5400 LCP.

## Compliance

The 5400 LCP is compliant with the following specifications:

- Telcordia Technologies GR-1089-CORE Sections 2, 3, 4, 5, 6, 7, 8, and 9
- Telcordia Technologies GR-63-CORE Sections 2, 3, 4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, and 4.7

# Eco-environmental statements

## Introduction

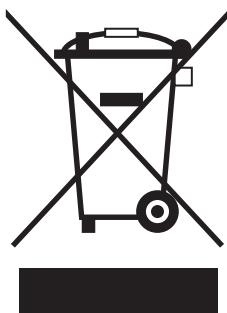
The statements that follow are the eco-environmental statements that apply to Alcatel-Lucent Technologies systems.

## Packaging collection and recovery requirements

Countries, states, localities, or other jurisdictions may require that systems be established for the return and/or collection of packaging waste from the consumer, or other end user, or from the waste stream. Additionally, reuse, recovery, and/or recycling targets for the return and/or collection of the packaging waste may be established.

## Recycling / take-back / disposal of product

Electronic products bearing or referencing the symbol shown below when put on the market within the European Union, shall be collected and treated at the end of their useful life in compliance with applicable European Union and local legislation. They shall not be disposed of as part of unsorted municipal waste. Due to materials that may be contained in the product, such as heavy metals or batteries, the environment and human health may be negatively impacted as a result of inappropriate disposal.



Note: In the European Union, a solid bar under the crossed-out wheeled bin indicates that the product was put on the market after 13 August 2005.

Moreover, in compliance with legal requirements and contractual agreements, where applicable, Alcatel-Lucent Technologies will offer to provide for the collection and treatment of Alcatel-Lucent Technologies products at the end of their useful life, or products displaced by Alcatel-Lucent Technologies equipment offers.

For information regarding take-back of equipment by Alcatel-Lucent Technologies, or for more information regarding the requirements for recycling/disposal of product, please contact your Alcatel-Lucent Account Manager or Alcatel-Lucent Takeback Support at [takeback@lucent.com](mailto:takeback@lucent.com) ([takeback@lucent.com](mailto:takeback@lucent.com)).

---

**Material Content Compliance**

European Union (EU) Directive 2002/95/EC, "Restriction of the use of certain Hazardous Substances" (RoHS), restricts the use of lead, mercury, cadmium, hexavalent chromium, and certain flame retardants in electrical and electronic equipment. This Directive applies to electrical and electronic products placed on the EU market from 1 July 2006, with various exemptions, including an exemption for lead solder in network infrastructure equipment. Alcatel-Lucent products shipped to the EU from 1 July 2006 will comply with the RoHS Directive.

# 12 Hazard statements

## Overview

### Purpose

This chapter provides all the safety warnings, dangers and cautions that apply to this manual.

### Contents

|                                |      |
|--------------------------------|------|
| Structure of safety statements | 12-2 |
| Common cautions and warnings   | 12-4 |
| Basic safety aspects           | 12-6 |

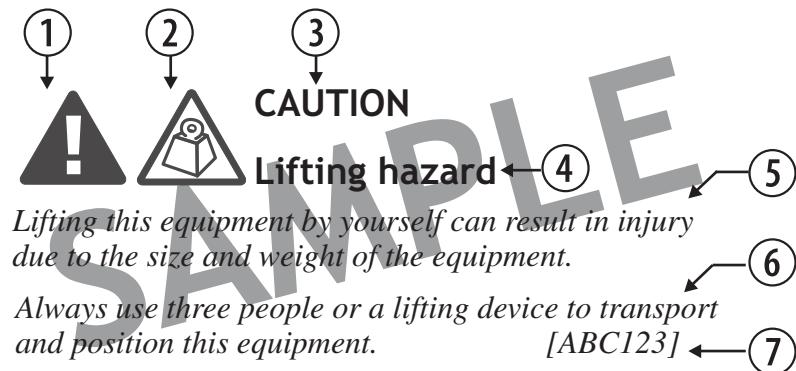
# Structure of safety statements

## Overview

This topic describes the components of safety statements that appear in this document.

## General structure

Safety statements include the following structural elements:



| Item | Structure element   | Purpose  |
|------|---------------------|--|
| 1    | Safety alert symbol | Indicates the potential for personal injury (optional) |
| 2    | Safety symbol       | Indicates hazard type (optional)                       |
| 3    | Signal word         | Indicates the severity of the hazard                   |
| 4    | Hazard type         | Describes the source of the risk of damage or injury   |
| 5    | Safety message      | Consequences if protective measures fail               |
| 6    | Avoidance message   | Protective measures to take to avoid the hazard        |
| 7    | Identifier          | The reference ID of the safety statement (optional)    |

---

**Signal words**

The signal words identify the hazard severity levels as follows:

| Signal word | Meaning   |
|-------------|---|
| DANGER      | Indicates an extremely hazardous situation which, if not avoided, will result in death or serious injury. |
| WARNING     | Indicates a hazardous situation which, if not avoided, could result in death or serious injury.           |
| CAUTION     | Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.          |
| NOTICE      | Indicates a hazardous situation not related to personal injury.   |

## Common cautions and warnings

### Common cautions



#### WARNING

##### Overhead-load hazard

*Cabinet eyebolts can break, severely damaging the cabinet, if a crane is used to lift the cabinet into an upright position.*

*Ensure that the cabinet is in an upright position before transportation by crane.*



#### WARNING

##### Electric-shock hazard

*There is a danger of electric shock if the grounding system is inadequate.*

*You must comply with the grounding requirements for the grounding system.*



#### CAUTION

##### Lifting hazard

*Lifting this equipment by yourself can result in injury due to the size and weight of the equipment.*

*Always use three people or a lifting device to transport and position this equipment.*



#### NOTICE

##### ESD hazard

*Electronic components can be destroyed by electrostatic discharge (ESD).*

*Circuit packs must therefore always be kept in antistatic covers. Use the original antistatic packaging if possible.*

*Always observe the general ESD instructions.*



#### NOTICE

##### Overhead-load hazard

*Connectors on the roof of the cabinet can be damaged during transport by the crane hook, lifting harness, or chains causing damage to the unit.*

*Avoid any contact between connectors and heavy lifting equipment. Operate with caution.*

**NOTICE****Service-disruption hazard**

*Condensation can occur in the network element during transport, especially on moving from outside to closed rooms. Condensation can cause malfunctioning of the circuit packs.*

*Ensure that circuit packs and shelves have reached room temperature and are dry before taking them into operation.*

All hazard statements that are not specific to individual procedures are mentioned here. Hazard statements describe risks, primarily to personnel, that are relevant to procedures that are performed during the deployment and/or use of Alcatel-Lucent products. Failure to avoid the hazards can have serious consequences.

# Basic safety aspects

## General safety requirements

To keep the technically unavoidable residual risk to a minimum, it is imperative to observe the following rules:

- Transport, storage, and operation of the system must be under *specified permissible conditions only*.

See the accompanying documentation and information on the system.

- Installation, configuration and disassembly must be carried out only by *suitably qualified personnel* and *with reference to the respective documentation*.

Due to the complexity of the system, personnel require *special training*.

- The system must be operated by *trained and authorized users only*.

The user must operate the system only after having *read and understood* the chapter on safety and the parts of the documentation relevant to operation. For complex systems, Alcatel-Lucent recommends additional training. Any obligatory training for operating and service personnel must be carried out and documented.

- Follow all instructions marked on the product, including both general instructions and the stated methods for avoiding hazards.

- The system must not be operated unless the safety is guaranteed. Any faults and errors that affect safety must be reported *immediately* by the user to a person in responsibility.

- Identify potential hazards *prior* to starting the installation.

- The system must be operated only with the connections and under the environmental conditions as described in the documentation.

- Modifications to any part of the system (including software) must be carried out by Alcatel-Lucent Technologies or by trained and qualified personnel authorized by Alcatel-Lucent Technologies.

Unauthorized modifications lead to *complete exemption from liability*.

Only components recommended by the manufacturer and listed in the procurement documents must be used.

- The use of non-system software is not recommended. The use/installation of non-system software can adversely affect the normal functioning of the system.

- Only use *tested and virus-free* data carriers (for example, floppy disks and streamer tapes).

- The removal or disabling of safety facilities, fault clearance and maintenance of equipment must be carried out by trained and qualified personnel only and in conjunction with the respective documentation. Only approved measuring and test equipment must be used.

- Calibrations, special tests after repairs and regular safety checks must be carried out, documented and archived.
- Only use specified chemicals or materials.
- Consult material safety data sheets (MSDS or equivalent) when working with hazardous chemicals.
- Follow applicable hazardous waste, electronic scrap, and take-back disposal procedures.

## Personal safety

Observe the following safety instructions, they are of particular importance for your safety:

- Be familiar with evacuation plans and emergency phone numbers.
- Ensure that first aid kits are available.
- Wear appropriate personal protective equipment (PPE) such as safety glasses, hard hats, gloves, and fall protection.
- Never wear jewelry, such as rings, bracelets, watches, when working on or near energized equipment.

## Summary of product safety instructions

Especially observe the following safety instructions, they are of particular importance for the equipment:

- The equipment is to be installed only in *Restricted Access Areas* in business and customer premises.  
Applications in accordance with Articles 110-16, 110-17 and 110-18 of the National Electrical Code, ANSI/NFPA No. 70, IEC 60215 and EN 60215 + A1. Other installations exempt from the enforcement of the National Electrical Code are engineered according to the accepted practices of the local telecommunications utility.
- The product must only be operated from the type of power source indicated on the marking label.
- The equipment must be provided with a readily accessible disconnect device as part of the building installation.
- Disconnect all power supply connections when removing power from the system.
- Installation must include an independent frame ground drop to the building ground. See the *Installation Guide* provided with the product.
- For information on proper cabinet mounting instructions, consult the *Installation Guide* provided with the product.
- Only install equipment identified in the *Installation Guide* provided with the product. Use of other equipment can result in improper connection of circuitry leading to fire or injury to persons.

- Slots and openings in the product are provided for ventilation. To protect the product from overheating, these openings must not be blocked or covered. Adequate clearances and ventilation must be provided as detailed in the Site Preparation Manual.
- Do not push objects of any kind into the product through slots. They can touch dangerous voltage points or short-out parts, and result in a risk of fire or electrical shock. Never spill liquids of any kind on the product.
- The equipment must be connected directly to:
  - the DC supply system grounding electrode conductor, or
  - to a bonding jumper from a grounding terminal bar or bus to which the DC supply system grounding electrode conductor is connected.
- The equipment must be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection between the grounded conductor of the same DC supply circuit and the grounding conductor, and also the point of grounding of the DC system. The DC system must not be grounded elsewhere.
- The DC supply source is to be located within the same premises as the equipment.
- There must be no switching or disconnection devices in the grounded circuit conductor between the DC source and the point of connection of the grounding electrode conductor.

# Appendix A: Sample output for fephGrowth -m

## Overview

This appendix provides a sample output of the **fephGrowth -m** command.

```
fephGrowth -m
fephGrowth: started 08/09/10 14:28
Verifying config host (10.82.194.0) is reachable
config host (10.82.194.0) ping test completed successfully
fephGrowth Process mapoffice request
Running su_health -a ...
#
#####Checking service type#####
service type cnfg, pool number 0
service type fs5k, pool number 0
service type fs5k, pool number 1
service type fsdb, pool number 0
service type h248, pool number 0
service type ims, pool number 0
service type ims, pool number 1
service type ims, pool number 2
service type ims, pool number 3
service type ims, pool number 4
service type ims, pool number 5
service type ims, pool number 6
service type ims, pool number 7
service type ims, pool number 8
service type ims, pool number 9
service type ims, pool number 10
service type ims, pool number 11
service type ims, pool number 12
service type ims, pool number 13
service type ims, pool number 14
service type ims, pool number 15
service type ims, pool number 16
service type mi, pool number 0
service type sns, pool number 0
#
#####Checking feature license#####


```

```
Dharma/isql Version 09.00.0000
Dharma Systems Inc (C) 1988-2003.
Dharma Systems Pvt Ltd (C) 1988-2003.
Both FEPH and iSGW-A are in feature license!
#
#####Checking IMS service #####
#
pool number 0; ims node 256; LABEL imsgroup0-000; NI type Default;
    External IP 010.223.009.038
pool number 0; ims node 256; LABEL imsgroup0-000; NI type Default;
    External IP 2802:5450:1:CA24::6
pool number 0; ims node 256; LABEL imsgroup0-000-b; NI type Published;
    External IP 135.001.183.043
pool number 0; ims node 256; LABEL imsgroup0-000-b; NI type Published;
    External IP 2802:5450:1:CA22::6
#
pool number 1; ims node 257; LABEL imsgroup0-001; NI type Default;
    External IP 010.223.009.039
pool number 1; ims node 257; LABEL imsgroup0-001; NI type Default;
    External IP 2802:5450:1:CA24::7
pool number 1; ims node 257; LABEL imsgroup0-001-b; NI type Published;
    External IP 135.001.183.044
pool number 1; ims node 257; LABEL imsgroup0-001-b; NI type Published;
    External IP 2802:5450:1:CA22::7
#
pool number 2; ims node 258; LABEL imsgroup0-002; NI type Default;
    External IP 010.223.009.040
pool number 2; ims node 258; LABEL imsgroup0-002; NI type Default;
    External IP 2802:5450:1:CA24::8
pool number 2; ims node 258; LABEL imsgroup0-002-b; NI type Published;
    External IP 135.001.184.041
pool number 2; ims node 258; LABEL imsgroup0-002-b; NI type Published;
    External IP 2802:5450:1:CA25::9
#
pool number 3; ims node 259; LABEL imsgroup0-003; NI type Default;
    External IP 010.223.009.041
pool number 3; ims node 259; LABEL imsgroup0-003; NI type Default;
    External IP 2802:5450:1:CA24::9
pool number 3; ims node 259; LABEL imsgroup0-003-b; NI type Published;
    External IP 135.001.183.046
pool number 3; ims node 259; LABEL imsgroup0-003-b; NI type Published;
    External IP 2802:5450:1:CA22::9
#
pool number 4; ims node 260; LABEL imsgroup0-004; NI type Default;
    External IP 010.223.009.042
pool number 4; ims node 260; LABEL imsgroup0-004; NI type Default;
    External IP 2802:5450:1:CA24::A
pool number 4; ims node 260; LABEL imsgroup0-004-b; NI type Published;
    External IP 135.001.183.047
pool number 4; ims node 260; LABEL imsgroup0-004-b; NI type Published;
    External IP 2802:5450:1:CA22::A
#
```

```

pool number 7; ims node 263; LABEL imsgroup0-007; NI type Default;
    External IP 010.223.009.045
pool number 7; ims node 263; LABEL imsgroup0-007; NI type Default;
    External IP 2802:5450:1:CA24::D
pool number 7; ims node 263; LABEL imsgroup0-007-b; NI type Published;
    External IP 135.001.184.036
pool number 7; ims node 263; LABEL imsgroup0-007-b; NI type Published;
    External IP 2802:5450:1:CA25::4
#
pool number 6; ims node 262; LABEL imsgroup0-006; NI type Default;
    External IP 010.223.009.044
pool number 6; ims node 262; LABEL imsgroup0-006; NI type Default;
    External IP 2802:5450:1:CA24::C
pool number 6; ims node 262; LABEL imsgroup0-006-b; NI type Published;
    External IP 135.001.184.035
pool number 6; ims node 262; LABEL imsgroup0-006-b; NI type Published;
    External IP 2802:5450:1:CA25::3
#
pool number 5; ims node 261; LABEL imsgroup0-005; NI type Default;
    External IP 010.223.009.043
pool number 5; ims node 261; LABEL imsgroup0-005; NI type Default;
    External IP 2802:5450:1:CA24::B
pool number 5; ims node 261; LABEL imsgroup0-005-b; NI type Published;
    External IP 135.001.184.034
pool number 5; ims node 261; LABEL imsgroup0-005-b; NI type Published;
    External IP 2802:5450:1:CA25::2
#
pool number 15; ims node 272; LABEL imsgroup0-015; NI type Default;
    External IP 010.223.009.053
pool number 15; ims node 272; LABEL imsgroup0-015; NI type Default;
    External IP 2802:5450:1:CA24::15
pool number 15; ims node 272; LABEL imsgroup0-015-b; NI type Published;
    External IP 135.001.184.039
pool number 15; ims node 272; LABEL imsgroup0-015-b; NI type Published;
    External IP
2802:5450:1:CA25::7
#
pool number 14; ims node 271; LABEL imsgroup0-014; NI type Default;
    External IP 010.223.009.052
pool number 14; ims node 271; LABEL imsgroup0-014; NI type Default;
    External IP 2802:5450:1:CA24::14
pool number 14; ims node 271; LABEL imsgroup0-014-b; NI type Published;
    External IP 135.001.184.038
pool number 14; ims node 271; LABEL imsgroup0-014-b; NI type Published;
    External IP
2802:5450:1:CA25::6
#
pool number 13; ims node 270; LABEL imsgroup0-013; NI type Default;
    External IP 010.223.009.051
pool number 13; ims node 270; LABEL imsgroup0-013; NI type Default;
    External IP 2802:5450:1:CA24::13
pool number 13; ims node 270; LABEL imsgroup0-013-b; NI type Published;
    External IP 135.001.184.037

```

```
pool number 13; ims node 270; LABEL imsgroup0-013-b; NI type Published;
    External IP
2802:5450:1:CA25::5
#
pool number 12; ims node 269; LABEL imsgroup0-012; NI type Default;
    External IP 010.223.009.050
pool number 12; ims node 269; LABEL imsgroup0-012; NI type Default;
    External IP 2802:5450:1:CA24::12
pool number 12; ims node 269; LABEL imsgroup0-012-b; NI type Published;
    External IP 135.001.183.055
pool number 12; ims node 269; LABEL imsgroup0-012-b; NI type Published;
    External IP
2802:5450:1:CA22::12
#
pool number 11; ims node 268; LABEL imsgroup0-011; NI type Default;
    External IP 010.223.009.049
pool number 11; ims node 268; LABEL imsgroup0-011; NI type Default;
    External IP 2802:5450:1:CA24::11
pool number 11; ims node 268; LABEL imsgroup0-011-b; NI type Published;
    External IP 135.001.184.043
pool number 11; ims node 268; LABEL imsgroup0-011-b; NI type Published;
    External IP
2802:5450:1:CA25::B
#
pool number 8; ims node 264; LABEL imsgroup0-008; NI type Default;
    External IP 010.223.009.046
pool number 8; ims node 264; LABEL imsgroup0-008; NI type Default;
    External IP 2802:5450:1:CA24::E
pool number 8; ims node 264; LABEL imsgroup0-008-b; NI type Published;
    External IP 135.001.183.051
pool number 8; ims node 264; LABEL imsgroup0-008-b; NI type Published;
    External IP 2802:5450:1:CA22::E
#
pool number 9; ims node 265; LABEL imsgroup0-009; NI type Default;
    External IP 010.223.009.047
pool number 9; ims node 265; LABEL imsgroup0-009; NI type Default;
    External IP 2802:5450:1:CA24::F
pool number 9; ims node 265; LABEL imsgroup0-009-b; NI type Published;
    External IP 135.001.183.052
pool number 9; ims node 265; LABEL imsgroup0-009-b; NI type Published;
    External IP 2802:5450:1:CA22::F
#
pool number 10; ims node 266; LABEL imsgroup0-010; NI type Default;
    External IP 010.223.009.048
pool number 10; ims node 266; LABEL imsgroup0-010; NI type Default;
    External IP 2802:5450:1:CA24::10
pool number 10; ims node 266; LABEL imsgroup0-010-b; NI type Published;
    External IP 135.001.184.042
pool number 10; ims node 266; LABEL imsgroup0-010-b; NI type Published;
    External IP
2802:5450:1:CA25::A
#
```

```

pool number 16; ims node 275; LABEL imsgroup0-016; NI type Default;
    External IP 010.223.009.037
pool number 16; ims node 275; LABEL imsgroup0-016; NI type Default;
    External IP 2802:5450:1:CA24::5
pool number 16; ims node 275; LABEL imsgroup0-016-b; NI type Published;
    External IP 135.001.184.040
pool number 16; ims node 275; LABEL imsgroup0-016-b; NI type Published;
    External IP
2802:5450:1:CA25::8
*****WARNING: There are no provisioned Sipia ports for ims
service node 256 ( pool number:
0 )*****
*****WARNING: There are no provisioned Sipia ports for ims
service node 264 ( pool number:
8 )*****
#
#####Checking PCSCF profiles in use#####
p-cscf profile id 3, IMS service node 258, pool number 2, P-CSCF Port
    number 5060
p-cscf profile id 3, IMS service node 263, pool number 7, P-CSCF Port
    number 5060
p-cscf profile id 3, IMS service node 262, pool number 6, P-CSCF Port
    number 5060
p-cscf profile id 3, IMS service node 261, pool number 5, P-CSCF Port
    number 5060
p-cscf profile id 3, IMS service node 272, pool number 15, P-CSCF Port
    number 5060
p-cscf profile id 3, IMS service node 271, pool number 14, P-CSCF Port
    number 5060
p-cscf profile id 3, IMS service node 270, pool number 13, P-CSCF Port
    number 5060
p-cscf profile id 3, IMS service node 268, pool number 11, P-CSCF Port
    number 5060
p-cscf profile id 3, IMS service node 266, pool number 10, P-CSCF Port
    number 5060
p-cscf profile id 3, IMS service node 275, pool number 16, P-CSCF Port
    number 5060
#####profile id 3#####
SECURE_SERVER_PORT = 0
SECURE_CLIENT_PORT1 = 0
SECURE_CLIENT_PORT2 = 0
SECURE_CLIENT_PORT3 = 0
SECURITY_GW_PROFILE_ID = 2
#
#####Checking Security Gateway Profile#####
#####Security gateway profile id 1#####
*****WARNING: There are no FEPH policies*****
#####Security gateway profile id 2#####
Trusted FEPH policy id is set to 4
#
#####Checking default gateway for ipv4#####

```

```

service type ims, pool number 0, member number 256, IPv4 subnet number 9
service type ims, pool number 1, member number 256, IPv4 subnet number 9
service type ims, pool number 10, member number 256, IPv4 subnet number
9
service type ims, pool number 11, member number 256, IPv4 subnet number
9
service type ims, pool number 12, member number 256, IPv4 subnet number
9
...
service type ims, pool number 5, member number 256, IPv4 subnet number 9
service type ims, pool number 6, member number 256, IPv4 subnet number 9
service type ims, pool number 7, member number 256, IPv4 subnet number 9
service type ims, pool number 8, member number 256, IPv4 subnet number 9
service type ims, pool number 9, member number 256, IPv4 subnet number 9
#
#####Checking default gateway for ipv6#####
service type fs5k, pool number 0, member number 256, IPv6 subnet number
6
service type fs5k, pool number 1, member number 256, IPv6 subnet number
6
service type ims, pool number 0, member number 256, IPv6 subnet number
10
service type ims, pool number 1, member number 256, IPv6 subnet number
10
service type ims, pool number 10, member number 256, IPv6 subnet number
10
service type ims, pool number 11, member number 256, IPv6 subnet number
10
service type ims, pool number 12, member number 256, IPv6 subnet number
10
...
service type ims, pool number 5, member number 256, IPv6 subnet number
10
service type ims, pool number 6, member number 256, IPv6 subnet number
10
service type ims, pool number 7, member number 256, IPv6 subnet number
10
service type ims, pool number 8, member number 256, IPv6 subnet number
10
service type ims, pool number 9, member number 256, IPv6 subnet number
10
#
#####Checking static route for ipv4#####
service type fs5k, pool number 0, member number 256, IPv4 subnet base
10.10.100.49, IPv4 subnet mask
255.255.255.255, IPv4 subnet number 2
service type fs5k, pool number 0, member number 256, IPv4 subnet base
10.10.100.51, IPv4 subnet mask
255.255.255.255, IPv4 subnet number 2
service type fs5k, pool number 0, member number 256, IPv4 subnet base
10.10.120.81, IPv4 subnet mask
255.255.255.255, IPv4 subnet number 4

```

```

service type fs5k, pool number 1, member number 256, IPv4 subnet base
  10.10.100.49, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 2
service type fs5k, pool number 1, member number 256, IPv4 subnet base
  10.10.100.51, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 2
service type fs5k, pool number 1, member number 256, IPv4 subnet base
  10.10.120.81, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 4
service type h248, pool number 0, member number 256, IPv4 subnet base
  10.10.100.49, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 2
service type h248, pool number 0, member number 256, IPv4 subnet base
  10.10.100.51, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 2
service type h248, pool number 0, member number 256, IPv4 subnet base
  10.10.120.119, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 4
...
service type ims, pool number 9, member number 256, IPv4 subnet base
  10.10.100.51, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 2
service type ims, pool number 9, member number 256, IPv4 subnet base
  10.10.120.115, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 4
service type ims, pool number 9, member number 256, IPv4 subnet base
  10.10.120.116, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 4
service type ims, pool number 9, member number 256, IPv4 subnet base
  10.10.120.117, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 4
service type ims, pool number 9, member number 256, IPv4 subnet base
  10.10.120.118, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 4
service type ims, pool number 9, member number 256, IPv4 subnet base
  10.10.120.119, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 4
service type ims, pool number 9, member number 256, IPv4 subnet base
  10.10.120.80, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 2
service type ims, pool number 9, member number 256, IPv4 subnet base
  10.10.120.82, IPv4 subnet mask
  255.255.255.255, IPv4 subnet number 2
#
#####Checking static route for ipv6#####
service type fs5k, pool number 0, member number 256, IPv6 subnet prefix
  2000::, IPv6 prefix length 3, IPv6
subnet number 6
service type fs5k, pool number 1, member number 256, IPv6 subnet prefix
  2000::, IPv6 prefix length 3, IPv6
subnet number 6

```

---

```

service type ims, pool number 0, member number 256, IPv6 subnet prefix
  2000::, IPv6 prefix length 3, IPv6
  subnet number 10
service type ims, pool number 0, member number 256, IPv6 subnet prefix
  2803:5450:1:a120:0:0:5a, IPv6
  prefix length 128, IPv6 subnet number 6
service type ims, pool number 0, member number 256, IPv6 subnet prefix
  2803:5450:1:a120:0:0:5b, IPv6
  prefix length 128, IPv6 subnet number 8
service type ims, pool number 0, member number 256, IPv6 subnet prefix
  2803:5450:1:a120:0:0:5c, IPv6
  prefix length 128, IPv6 subnet number 6
service type ims, pool number 1, member number 256, IPv6 subnet prefix
  2000::, IPv6 prefix length 3, IPv6
  subnet number 10
service type ims, pool number 1, member number 256, IPv6 subnet prefix
  2803:5450:1:a120:0:0:5a, IPv6
  prefix length 128, IPv6 subnet number 6
service type ims, pool number 1, member number 256, IPv6 subnet prefix
  2803:5450:1:a120:0:0:5b, IPv6
  prefix length 128, IPv6 subnet number 8
...
service type ims, pool number 8, member number 256, IPv6 subnet prefix
  2000::, IPv6 prefix length 3, IPv6
  subnet number 10
service type ims, pool number 8, member number 256, IPv6 subnet prefix
  2803:5450:1:a120:0:0:5a, IPv6
  prefix length 128, IPv6 subnet number 6
service type ims, pool number 8, member number 256, IPv6 subnet prefix
  2803:5450:1:a120:0:0:5b, IPv6
  prefix length 128, IPv6 subnet number 8
service type ims, pool number 8, member number 256, IPv6 subnet prefix
  2803:5450:1:a120:0:0:5c, IPv6
  prefix length 128, IPv6 subnet number 6
service type ims, pool number 9, member number 256, IPv6 subnet prefix
  2000::, IPv6 prefix length 3, IPv6
  subnet number 10
service type ims, pool number 9, member number 256, IPv6 subnet prefix
  2803:5450:1:a120:0:0:5a, IPv6
  prefix length 128, IPv6 subnet number 6
service type ims, pool number 9, member number 256, IPv6 subnet prefix
  2803:5450:1:a120:0:0:5b, IPv6
  prefix length 128, IPv6 subnet number 8
service type ims, pool number 9, member number 256, IPv6 subnet prefix
  2803:5450:1:a120:0:0:5c, IPv6
  prefix length 128, IPv6 subnet number 6
#
#####Checking external subnet for ipv4#####
IPv4 subnet number 1, subnet base 10.223.8.32, subnet mask
  255.255.255.224, subnet name OAM
IPv4 subnet number 2, subnet base 135.1.183.32, subnet mask
  255.255.255.224, subnet name SIGAccess

```

---

```
IPv4 subnet number 3, subnet base 10.223.9.32, subnet mask  
255.255.255.224, subnet name SIGCore  
IPv4 subnet number 4, subnet base 10.223.7.32, subnet mask  
255.255.255.224, subnet name Billing  
IPv4 subnet number 9, subnet base 135.1.184.32, subnet mask  
255.255.255.224, subnet name SigDHSP4  
#  
#####Checking external subnet for ipv6#####  
IPv6 subnet number 10, subnet prefix 2802:5450:1:ca25:0:0:0:0, prefix  
length 64, subnet name Sig6DHSP4  
IPv6 subnet number 5, subnet prefix 2802:5450:1:ca21:0:0:0:0, prefix  
length 64, subnet name OAM6  
IPv6 subnet number 6, subnet prefix 2802:5450:1:ca22:0:0:0:0, prefix  
length 64, subnet name SIG6Access  
IPv6 subnet number 7, subnet prefix 2802:5450:1:ca24:0:0:0:0, prefix  
length 64, subnet name SIG6Core  
IPv6 subnet number 8, subnet prefix 2802:5450:1:ca23:0:0:0:0, prefix  
length 64, subnet name Billing6  
#  
The result is in /var/opt/log/fephGrowth/mapOffice.txt  
fephGrowth: Completed Successfully.  
fephGrowth ended 08/09/10 14:30
```



# Appendix B: References

## Overview

### Purpose

This appendix provides the revision history of the *5450 IP Session Control Provisioning Guide*.

### Contents

|                 |     |
|-----------------|-----|
| Reissue history | B-1 |
|-----------------|-----|

# Reissue history

## Purpose

The reissue history of this document is described in the following paragraphs.

### Issue 0.02

The revision history for Issue 0.02 is shown in the following table.

**Table B-1 Issue 0.02, June 2012**

| Location   | Change  |
|--|---|
| “Support multiple access network subnets on FEPH” (p. 5-342)                                   | Newly added topic as part of SEAL Ph6 - Support Multiple Access Network Subnets on FEPH.                                |
| “To grow a new external access subnet” (p. 5-343)  | Newly added topic as part of SEAL Ph6 - Support Multiple Access Network Subnets on FEPH.                                |
| “To convert one ordinary subnet to external access subnet” (p. 5-360)                          | Newly added topic as part of SEAL Ph6 - Support Multiple Access Network Subnets on FEPH.                                |
| “To degrow one external access subnet” (p. 5-371)  | Newly added topic as part of SEAL Ph6 - Support Multiple Access Network Subnets on FEPH.                                |
| “To provision the Service Based Local Policy Profile” (p. 4-111)                               | Updated the topic. Added a new parameters as part of feature, “Enhance MSRP Support for MMIM server and UE behind NAT”. |
| “Provisioning Task flow - To support new versions of IMS charging SPEC 3GPP 32.260” (p. 1-127) | Newly added topic as part of feature, “Support New Versions of IMS Charging SPEC 3GPP 32.260”.                          |
| “To provision an ACR Charging Profile” (p. 8-5)  | Updated the topic. Added new parameters as part of feature, “Support New Versions of IMS Charging SPEC 3GPP 32.260”.    |

**Table B-1 Issue 0.02, June 2012 (continued)**

| Location   | Change   |
|--|--|
| “To add an H.248 Device Server” (p. 7-29)  | Updated the topic. Added new parameters as part of feature, “Support New Versions of IMS Charging SPEC 3GPP 32.260”.   |
| “To provision a Diameter profile” (p. 10-23)   | <p>Updated the topic.</p> <p>Added new parameters as part of the following features:</p> <ul style="list-style-type: none"> <li>• Diameter support of DPR/DPA messages</li> <li>• Origin-Host /Origin-Realm AVPs Setting in Diameter Application Message</li> <li>• Configurable DSCP Marking for Diameter Messages</li> <li>• Support Primary and Alternate SLF Destination for Geo-Redundancy</li> </ul> |
| “To provision an S-CSCF profile” (p. 4-15)   | Updated the topic. Added new parameters as part of feature, “S-CSCF sending default PUID to AS for PBX trunking services”.   |
| “Provisioning task flow - To provision primary and alternate SLF destination for geo-redundancy support ” (p. 1-125) | Newly created topic as part of feature, “Support Primary and Alternate SLF Destination for Geo-Redundancy”.  |
| “To provision a Diameter Multiple Destination Profile” (p. 4-278)  | Updated the topic. Added new parameters as part of feature, “Support Primary and Alternate SLF Destination for Geo-Redundancy”.  |
| “Provisioning Task flow - To provision SIP heartbeat after failure to reach a network element” (p. 1-123)            | Newly created topic as part of feature, “SIP heartbeat after failure to reach a network element”.  |
| “To provision NGSS Server parameters” (p. 10-9)  | Updated the topic. Added new parameters as part of feature, “SIP heartbeat after failure to reach a network element”.  |

**Table B-1 Issue 0.02, June 2012 (continued)**

| Location  | Change  |
|---|---|
| “To provision a SIPia port” (p. 10-40)  | Updated the topic. Added new parameters as part of feature, “SIP heartbeat after failure to reach a network element”.   |
| “To provision PCSCF profile” (p. 4-77)  | Updated the topic. Added new parameters as part of feature, “SIP heartbeat after failure to reach a network element”.<br>Updated the topic. Added a new parameter as part of feature, “Support of Service-URN AVP for Rx Interface”. This feature supports inclusion of the Service-URN AVP in the Rx interface to ensure that the PCRF identifies this as an emergency call and therefore allows the call to be setup over the emergency bearer. |
| “To provision an SIP Heartbeat after failure Exemption Table” (p. 5-337)                  | Newly created topic as part of feature, “SIP heartbeat after failure to reach a network element”.   |
| “To provision an ACR Charging Profile” (p. 8-5)   | Updated the topic to add the provisioning of the Allow ABF flag   |
| “Provisioning Task flow - To provision S-CSCF pool” (p. 4-40)                             | Added the topic to describe the provisioning task flow of the feature “S-CSCF Pool”   |
| “To provision NGSS Server parameters” (p. 10-9)<br>“To provision ICSCF Profile” (p. 4-45) | Updated the topics to add provisioning related to “S-CSCF Pool”   |
| “Provisioning Task flow - To provision P-CSCF pool” (p. 4-126)                            | Added the topic to describe the provisioning related to “P-CSCF pool”   |
| “To provision NGSS Server parameters” (p. 10-9)   | Updated the topic to add provisioning related to “P-CSCF Pool”  |

**Table B-1 Issue 0.02, June 2012 (continued)**

| <b>Location</b>   | <b>Change</b>  |
|---|--|
| “To provision Service-Based PCSCF Profile” (p. 4-69)            | Updated the topics to add provisioning related to “3GPP IBC enhancement”               |
| “To provision NGSS Server parameters” (p. 10-9)                 |  |
| “To provision a Session Description Protocol Profile” (p. 4-62) | Updated the topics to add provisioning related to “IBC Support Multiple AMR Rate Sets” |



# Glossary

## Numerics

### 3GPP

Third-Generation Partnership Project

## A A-RACF

Access–Resource and Admission Control Function

### AAA

Authentication, Authorization, and Accounting

### ABF

ACR Buffering Function

### ACK

Acknowledgement

### ACL

Answer Code List

### ACR

Anonymous Call Rejection

### ACR

Accounting Request

### AKA

Authentication and Key Agreement

### ALG

Application Level Gateway

### ALG

Application Layer Gateway

### AP

Access point

**AS**

Autonomous system

**AS**

Application Server

**ATA**

Advanced Technology Attachment

**ATA**

Analog Terminal Adaptor

**ATCF**

Access Transfer Control Function

**ATGW**

Access Transfer Gateway

**AuCL**

Auxiliary Codec List

**AUTN**

Authentication

**AVP**

Attribute Value Pair

**AXAS**

Address eXchange Application Server

**B****B2BUA**

Back-to-Back User Agent

**BEPH**

Back-End Packet Handler

**BGC**

Boredr Gateway Controller

**BGCF**

Border Gateway Control Function

**BGCF**

Breakout Gateway Control Function

**BWAS**

BroadWorks Application Server

**BWNS**

BroadWorks Network Server

**C CCCF**

Call Continuity Control Function

**CCF**

Conditional Call Forwarding

**CCF**

Call Control Function

**CCF**

Charging Collection Function

**CCR**

Credit Control Request

**CDF**

Combined Distribution Frame

**CDF**

Charging Data Function

**CdPN**

Called Party Number

**CgPN**

Calling Party Number

**CIC**

Circuit Identification Code

**CIC**

Carrier Identification Code

**CK**

Cyphering Key

**CK**

Confidentiality Key

**CLF**

Connectivity Session Location and Repository Function

**CLIP**

Calling Line Identification Presentation

---

|             |                                    |
|-------------|------------------------------------|
| <b>CP</b>   | Call Processing                    |
| <b>CPC</b>  | Calling Party Category             |
| <b>CRLF</b> | Carriage-Return Line-Feed sequence |
| <b>CS</b>   | Circuit Switched                   |
| <b>CS</b>   | Call Server                        |
| <b>CSV</b>  | Comma-Separated Value              |
| <b>CTF</b>  | Charging Trigger Function          |
| <b>CTS</b>  | Converged Telephony Server         |
| <b>CW</b>   | Call Waiting                       |

---

|          |             |                                     |
|----------|-------------|-------------------------------------|
| <b>D</b> | <b>DA</b>   | Digit Analysis                      |
|          | <b>DB</b>   | Database                            |
|          | <b>DF</b>   | Delivery Function                   |
|          | <b>DF</b>   | Data Fanout                         |
|          | <b>DHCP</b> | Dynamic Host Configuration Protocol |
|          | <b>DNS</b>  | Domain Name System                  |
|          | <b>DS</b>   | Device Server                       |

**DSL**

Digital Subscriber Line

**E E-CSCF**

Emergency Call Session Control Function

**EATF**

Emergency Access Transfer Function

**ECF**

Event Charging Function

**ECUR**

Event Charging with Unit Reservation

**EDAS**

Extended Digit Analysis Application Server

**EEAS**

E.164 Expansion Application Server

**ENUM**

E.164 Number to URI Mapping

**ENUM**

Telephone Numbering Mapping

**ESD**

Electrostatic Discharge

**ESGW**

Emergency Service Gateway

**ESP**

Encapsulating Security Payload

**ESP**

External Security Password

**ESQK**

Emergency Services Query Key

**ESRN**

Emergency Services Routing Number

**eSRVCC**

Enhanced Single Radio Voice Call Continuity (domain transfer from LTE to a CS domain controlled by the ATCF in the Visited IMS network).

**EU**

European Union

**F FEPH**

Front-End Packet Handler

**FQDN**

Fully-Qualified Domain Name

**FS**

Feature Server

**G GCL**

Golden Codec List

**GGSN**

Gateway GPRS Support Node

**GLS**

Geographic Location Server

**GUI**

Graphical User Interface

**GUL**

Generic URI Label

**GWF**

Gateway Function

**H HOAS**

HandOver Application Server

**HSS**

Home Subscriber Server

**HTTP**

Hypertext Transfer Protocol

|             |  |
|-------------|--|
| <b>I</b>    | <b>I-CSCF</b><br>Interrogating Call Session Control Function |
| <b>IBCF</b> | Interconnection Border Control Function                      |
| <b>ICID</b> | IMS Charging IDentifier                                      |
| <b>ICMP</b> | Internet Control Message Protocol                            |
| <b>ICS</b>  | IMS Centralized Services                                     |
| <b>IEC</b>  | Immediate Event Charging                                     |
| <b>IEC</b>  | International Electrotechnical Commission                    |
| <b>IETF</b> | Internet Engineering Task Force                              |
| <b>iFC</b>  | initial Filter Criteria                                      |
| <b>IK</b>   | Integrity Key  |
| <b>IM</b>   | IP Multimedia  |
| <b>IM</b>   | Inventory Management   |
| <b>IM</b>   | Instant Messaging  |
| <b>IM</b>   | Input Message  |
| <b>IMPI</b> | IP Multimedia Private Identity                               |
| <b>IMS</b>  | IP Multimedia Subsystem                                      |

**IMSI**

International Mobile Subscriber Identity

**IMUX**

IMS Multiplexer

**IOI**

Inter Operator Identifier

**IP**

Intelligent Peripheral

**IP**

Internet Protocol

**IPSec**

Internet Protocol Security

**IRS**

Implicit Registration Set

**ISC**

Internet Service Consortium

**ISC**

IP Multimedia Service Control

**ISGW**

integrated Security Gateway

**ISIM**

IMS Subscriber Identity Module

**ISUP**

ISDN User Part

**L LAN**

Local Area Network

**LCP**

Linux Control Platform

**LDAC**

Load Distribution - Admission Control

**LI**

Lawful Intercept

---

**LI**

Line Interface

**LIA**

Location Information Answer

**LIR**

Location Information Request

**LTE**

Long Term Evolution

**LVAS**

Alcatel-Lucent Voice Application Server

**LZD**

Local Zone Domain

---

**M MD5**

Message Digest 5

**MG**

Media Gateway

**MGCF**

media gateway control function

**MMAS**

Mobility Management Application Server

**MRF**

Media Resource Function

**MSN**

Multiple Subscriber Number

**MSRP**

Message Session Relay Protocol

---

**N NAPTR**

Naming Authority Pointer

**NASS**

Network Attachment Subsystem

**NBA**

NASS Bundled Authentication

**NeDS**

Network Domain Selection

**NENA**

National Emergency Number Association

**NGSS**

next-generation SIP server

**NI**

Number Incomplete

**NI**

Network Interface

**O OCF**

Online Charging Function

**OCL**

Offer Codec List

**OCS**

Online Charging System

**ODM**

Office Data Manual

**OMC-P**

Operations and Maintenance Center - P

**OOS**

Out Of Service

**P P-CSCF**

Proxy CSCF

**P-NAPTR**

Pseudo Network Address Pointer

**PAID**

P-Asserted-IDentity SIP header

**PCRF**

Policy Charging Rules Functions

**PD-FE**

Policy Decision Functional Entity

**PDF**

Policy Decision Function

**PDF**

Power Distribution Frame

**PDP**

Policy Decision Point

**PDP**

Private Dial Plan

**PDP**

Packet Data Protocol

**PEP**

Policy Enforcement Point

**PPE**

Personal Protective Equipment

**PRID**

Private User Identity

**PS**

Presence Server

**PSAP**

Public Safety Answering Point

**PSI**

Public Service Identity

**PSTN**

Public Switched Telephone Network

**PUID**

Public User Identity

**Q**

**QoS**

Quality of Service

**R****RACS**

Resource and Admission Control Subsystem

**RAND**

Random Challenge

**RCEF**

Resource Control Enforcement Function

**RCI**

Registry Cache Index

**RES**

response

**RoHS**

Restriction of the use of certain Hazardous Substances

**RR**

Record-Route header

**S****S-CSCF**

Serving CSCF

**S-CSCF**

Serving Call Session Control Function

**SA**

Security Association

**SAP**

Service Access Point

**SAR**

Server Assignment Request

**SBBC**

Service-Based Bearer Control

**SBC**

Session Border Controller

**SBLP**

Service Based Local Policy

**SCC AS**

Service Centralization and Continuity Application Server

**SCG AS**

Service Continuity Gateway AS – 5420 SCG AS is ALU product for SCC AS functions

**SCTP**

Stream Control Transmission Protocol

**SCUR**

Session Charging with Unit Reservation

**SDP**

Session Description Protocol

**SEAL**

Secure External Access Lockout

**SiFC**

Shared initial Filter Criteria

**SigComp**

Signaling Compression

**SIP**

Session Initiation Protocol

**SIPia**

SIP Internal API

**SL**

Service Label

**SM**

State Machine

**SMS**

Short Message Service

**SMS**

Service Management System

**SPDF**

Service Policy Decision Function

**SPDF**

Service-based Policy Decision Function

**SPT**

Service Point Trigger

**SR**

Service-Route header

**SRVCC**

Single Radio Voice Call Continuity (domain transfer from IMS domain / LTE Access Network to a CS domain)

**STI**

Session Transfer Identifier

**STN**

Session Transfer Number

**STN-SR**

Session Transfer Number for Single Radio

**STR**

Session Termination Request

**STUN**

Simple Traversal of User Datagram Protocol

**T TCP**

Transmission Control Protocol

**THIG**

Topology Hiding Inter-network Gateway

**TISPAN**

Telecommunications and Internet Converged Services and Protocols

**TLDN**

Temporary Local Directory Number

**TPF**

Traffic Plane Function

**TU**

Transaction User

**U UA**

User Agent

**Glossary****UDA**

User Data Answer

**UDP**

User Datagram Protocol

**UDR**

User Data Request

**UE**

User Equipment

**URI**

Uniform Resource Identifier

**USDS**

Unified Subscriber Data Server

**USIM**

UMTS Subscriber Identity Module

**USSD**

Unstructured Supplementary Service Data

**V****VG**

Virtual Group

**VLAN**

Virtual Local Area Network

**VoIP**

Voice over Internet Protocol

**VoWLAN**

Voice over WLAN

**VPC**

VoIP Positioning Center

**X****XML**

Extensible Markup Language

**XRES**

Expected Authentication Response

**XSP**

Extensible Server Pages

# Index

## Numerics

3GPP2 SBBC

configuration flow, [2-3](#)

## A ABF

Provisioning task flow, [3-5](#)

ABF Provisioning

Add, modify or delete a Diameter profile, [8-24](#)

Access border for Pre-IMS core provisioning task flow, [1-104](#)

ACR

provisioning task flow, [3-3](#)

ACR Buffering Function

ABF, [8-21](#)

ACR Consolidation enhancement, [8-18](#)

ACR message generation

SIPia port, [8-3](#)

Activate

CDMA access network information, [8-30](#)

activate

Enhanced third party registration, [4-35](#)

PacketCable authentication - P-CSCF, [4-104](#)

Activate

PacketCable authentication - S-CSCF, [4-29](#)

Add

IMS Service association, [10-20](#)

incoming digit table attributes, [10-50](#)

add FEPH capability for IMS service, [5-167](#)

Add or delete an NTM Exemption table, [4-226](#)

Add, modify or delete a P-CSCF profile

IMS signaling security, [4-108](#)

Add, modify or delete an I-CSCF profile, [4-230](#)

Add, modify or delete an NTM Control table, [4-222](#)

Add, modify or delete an S-CSCF profile

IMS signaling security, [4-108](#)

Add, modify or delete an SIP Flow Trusted/Untrusted Rate Limit Rule Set, [5-68](#)

add, modify, or delete

SIP Permanent Linkset Group, [4-269](#)

Add, modify, or delete a BGCF local number Digit Analysis route table, [4-181](#)

Add, modify, or delete a BGCF location based routing table, [4-189](#)

Add, modify, or delete an Online Charging profile, [9-3, 9-7](#)

Additional ACR control, [8-15](#)

AKA

IMS signaling security, [4-108](#)

Alcatel-Lucent Session manager

Early IMS Security provisioning task flow, [1-41](#)

I-CSCF provisioning taskflow, [1-12](#)

P-CSCF provisioning task flow, [1-15](#)

S-CSCF provisioning task flow, [1-7](#)

Allow SIPS-URI on Gm and Mw Interface, [1-84](#)

## B Base Configuration

Execute, [10-6](#)

Bearer Statistics Collection on iAGCF., [1-59](#)

BGCF

release codes for 5420 CTS, [6-7](#)

|  |   |   |
|--|---|---|
| BGCF provisioning  | create PSI sub-domain list, <a href="#">4-57</a>  | Emergency provisioning scenarios, <a href="#">4-205</a>                   |
| BGCF CIC dialing prefix, <a href="#">6-4</a>                                     | Cx Enhancement to support SIP Digest per 3GPP R8 - Provisioning task flow, <a href="#">1-66</a> | Enhanced third party registration activate, <a href="#">4-35</a>          |
| BGCF per-carrier translation, <a href="#">6-5</a>                                |   | Enhancement of Rx and Gq' interfaces - Provisioning, <a href="#">1-83</a> |
| BGCF sample translations, <a href="#">6-6</a>                                    |   | External Domain Routing table   |
| BGCF support for Digit Manipulation provisioning task flow, <a href="#">1-73</a> | D default gateway and static routes for IMS services, <a href="#">5-162</a>                     | To provision an External Domain Routing table, <a href="#">10-99</a>      |
| BGCF translations, <a href="#">6-3</a>   | Delete  | external subnets, <a href="#">5-160</a>                                   |
| Block nomadic user access  | IMS Service association, <a href="#">10-20</a>  |   |
| Enable/disable, <a href="#">5-7</a>  | incoming digit table attributes, <a href="#">10-50</a>  |   |
|  | Device server (H.248)   |   |
|  | Component provisioning, <a href="#">7-29</a>  |   |
| C cautions and warnings, <a href="#">12-4</a>                                    | Diameter  |   |
| Change operational state of a SIPia port, <a href="#">10-80</a>                  | Add, modify or delete a Service to Diameter mapping, <a href="#">10-32</a>                      |   |
| charging, <a href="#">8-15</a>   | Diameter on host, <a href="#">10-32</a>   |   |
| Charging   | Diameter on NGSS, <a href="#">10-32</a>   |   |
| P-CSCF, <a href="#">8-30</a>   | Modify application IDs, <a href="#">10-31</a>   |   |
| charging profile assignment, <a href="#">8-15</a>                                | To provision Diameter profile, <a href="#">10-23</a>  |   |
| CLF  | Diameter port   |   |
| provisioning, <a href="#">4-116</a>  | Lock, or unlock, <a href="#">10-111</a>   |   |
| CMCC Emergency Service and P-CSCF SIP Header                                     | Digit Analysis (DA) Rules, <a href="#">5-98</a>   |   |
| Manipulation provisioning task flow, <a href="#">1-78</a>                        | Digit Analysis (DA) Rules -BGCF, <a href="#">5-105</a>  |   |
| Compliance   | Digit string  |   |
| RoHS, <a href="#">11-3</a>   | wildcards, <a href="#">10-68</a>  |   |
| WEEE, <a href="#">11-3</a>   | disable FEPH on FEPH-enabled IMS service, <a href="#">5-166</a>                                 |   |
| Compliance summary   |   |   |
| LCP 5400, <a href="#">11-2</a>   |   |   |
| Conversion   | E e2 interface support  |   |
| Diameter Connection Interface, <a href="#">4-273, 4-276</a>                      | task flow, <a href="#">4-116</a>  |   |
| Diameter Geo-redundancy, <a href="#">4-276</a>                                   | Eco-environmental   |   |
| Multiple Destinations, <a href="#">4-273</a>                                     | statement, <a href="#">11-3</a>   |   |

|   |  |   |
|---|--|---|
| view operational state, <a href="#">10-82</a>   | Multiple Destination FQDNs                                   | Provision   |
| IMS Service Growth with an existing FEPH Service, <a href="#">5-163</a>                               | provisioning task flow, <a href="#">1-36</a>                 | AGCF CPC String to CPC Digit Table, <a href="#">5-328</a>             |
| ims_cli, <a href="#">10-84</a>  | <b>N</b> NASS-bundled authentication                         | provision   |
| IMS-GWF   | provisioning task flow, <a href="#">1-43</a>                 | AGCF SIP Error Code To H248 Tone Table, <a href="#">5-246</a>         |
| provisioning task flow, <a href="#">1-30</a>  | <b>O</b> online charging                                     | Provision   |
| Introduction to Digit Analysis (DA) tables, <a href="#">5-95</a>                                      | S-CSCF profil, <a href="#">9-7</a>                           | Aggregate Source Address Policy, <a href="#">5-80</a>                 |
| IP Session Control  | Online Charging profile, <a href="#">9-3</a>                 | Application Layer Policy, <a href="#">5-87</a>                        |
| BGCF provisioning task flow, <a href="#">1-19</a>   | <b>P</b> P-CSCF  | provision   |
| configuration flow, <a href="#">1-5</a>   | Profile compression provisioning, <a href="#">4-106</a>      | BGCF DA Route Table, <a href="#">4-172</a>                            |
| E-CSCF provisioning taskflow, <a href="#">1-25</a>  | Profile provisioning, <a href="#">4-102</a>                  | BGCF Default Network Gateway, <a href="#">4-156</a>                   |
| EEAS provisioning task flow, <a href="#">1-28</a>   | Service Based Local Policy, <a href="#">4-111</a>            | BGCF Network Gateway, <a href="#">4-152</a>                           |
| iAGCF provisioning taskflow, <a href="#">1-33</a>   | PacketCable authentication - P-CSCF                          | BGCF Originating Host ID, <a href="#">4-193</a>                       |
| NTM provisioning task flow, <a href="#">1-27</a>  | activate, <a href="#">4-104</a>                              | BGCF Profile, <a href="#">4-142</a>                                   |
| IPSec   | PacketCable authentication - S-CSCF                          | BGCF SIP Content Type, <a href="#">4-177</a>                          |
| IMS signaling security, <a href="#">4-108</a>   | activate, <a href="#">4-29</a>                               | BGCF Target List, <a href="#">4-138</a>                               |
| <b>L</b> Limit for TCP Connections - Provisioning, <a href="#">1-82</a>                               | PD-FE Policy Provisioning                                    | BGCF Time Of Day, <a href="#">4-148</a>                               |
| <b>M</b> Media Inactivity provisioning task flow, <a href="#">2-16</a>                                | 3GPP2, <a href="#">2-6</a>                                   | BGCF URI Id, <a href="#">4-133</a>                                    |
| Migration Procedure for Signaling Firewall Load Balancer/Distribution Function, <a href="#">5-223</a> | TISPAN, <a href="#">2-15</a>                                 | CANM Profile Table, <a href="#">5-239</a>                             |
| Modify  | PPL components   | Provision   |
| IMS Service association, <a href="#">10-20</a>  | Provisioning, <a href="#">10-116</a>                         | client access to the Geographic Location Server, <a href="#">5-15</a> |
| incoming digit table attributes, <a href="#">10-50</a>  | provision  | provision   |
|   | a Core Bearer Realm, <a href="#">4-283</a>                   | Default Access Location Table, <a href="#">5-259</a>                  |
|   | a P-NAPTR Region, <a href="#">4-253</a>                      | Diameter Multiple Destination Profile, <a href="#">4-278</a>          |
|   | a Published Realm, <a href="#">4-286</a>                     | Provision   |
|   | Access Location to ESRN Mapping Table, <a href="#">5-250</a> | Diameter port, <a href="#">10-108</a>                                 |
|   | ACL List, <a href="#">5-322</a>                              | Emergency Identifiers List, <a href="#">5-61</a>                      |

|   |   |   |
|---|---|---|
| Flow Source Address Policy, 5-76                | P-NAPTR Target URI, 4-257                                 | provision   |
| Geographic Location Server, 5-13                | PBX Table entry, 4-96                                     | SIP forking, 1-40   |
| provision                                       | PCSCF Profile, 4-77                                       | Provision   |
| Home Network Identifier Profile table, 4-33     | Provision   | SIP Heartbeat after failure                                 |
| IBC Domain Table, 5-314                         | PDF profile, 10-104                                       | Exemption Table, 5-337                                      |
| IBC Route Profile, 5-297                        | provision   | provision   |
| IBC-A Profile, 5-290                            | Published NI Group Assignment table, 5-230                | SIP Linkset, 4-264  |
| IBC-A VG Policy, 5-133                          | Provision   | SIP Stack Timer Profile, 4-74                               |
| IBCF Profile, 4-198                             | Registration Failure Policy, 5-83                         | Provision   |
| ICSCF Profile, 4-45                             | provision   | STN-SR Table, 5-332   |
| ICSI profile, 5-117                             | Remote IP Policy Table, 5-266                             | provision   |
| IGWF profile, 4-250                             | S-CSCF PSI URI, 4-31                                      | Target Group, 5-304   |
| IMS Digit Table, 5-110                          | SDP Media MSRP Table, 5-286                               | Target Group List, 5-310                                    |
| IMS Emergency Service Identifier, 4-208         | SDP Profile, 4-62   | TLS Profile Attributes, 4-121                               |
| IMUX Port, 5-274                                | Provision   | Provision   |
| IMUX to IMS Association Table, 5-271            | Security Gateway profile, 5-90                            | To provision S-Cscf Capability List, 4-53                   |
| IP Address Mapping Table, 5-255                 | provision   | provision   |
| Provision                                       | Service Level Policy, 5-129                               | Treatment Trigger Data Table, 5-236                         |
| MACAddress to Location table entries, 5-9, 5-11 | Service-Based PCSCF Profile, 4-69                         | Trunk Group, 5-318  |
| provision                                       | Session Description Protocol Profile, 4-62                | VG and Service Mapping Profile, 5-137                       |
| MRF Announcement Data table, 4-247              | Provision   | Virtual Group profile, 5-125                                |
| MRF Announcement Interface profile, 4-245       | SIP Aggregate Trusted/Untrusted Rate Limit Rule Set, 5-72 | Provision an Aggregate Flow Policy, 5-150                   |
| Provision                                       | provision   | Provision an Aggregate Packet Policy, 5-147                 |
| NGN GETS Identifier List, 5-64                  | SIP Error Code table, 5-106                               | Provision an Aggregate Policy Assignment, 5-154             |
| provision                                       | Provision   | Provision Common Announcement Module (CANM) task flow, 1-69 |
| Online Charging Data table, 4-242               | SIP Filter Parameter Rule, 5-50                           | provision CRF target table, 4-297                           |
|   | SIP Filter Reference Rule, 5-44                           | Provision ENUM server address, 10-49                        |
|   | SIP Filter Set, 5-57                                      |   |

- 
- Provision iAGCF support of Network Traffic Management (NTM), [1-75](#)
- Provision Integrated Security Gateway (iSGW), [1-51](#)
- Provision inter-working of media between IPv4 and IPv6 networks, [1-46](#)
- Provision P-CSCF support of generating ACRs for emergency calls, [1-53](#)
- Provision the S-CSCF profile to support IP-PBX calls, [4-36](#)
- Provision the Signaling Firewall, [1-62](#)
- Provision the support of session and bandwidth limits per enterprise/PBX, [1-60](#)
- provisioning
- CLF, [4-116](#)
  - TISPAN RACS, [2-9](#)
- Provisioning - iAGCF Line OOS and CPC Display functionalities, [1-119](#)
- Provisioning - S-CSCF Assisted Relocation Procedure for Geo-Redundancy Enhancement, [1-118](#)
- Provisioning - Support ATCF, [1-121](#)
- Provisioning - Support MSRP Peak Data Rate to Enhance User Experience, [1-94](#)
- Provisioning Cx Enhancement per 3GPP R7 and R8, [1-68](#)
- Provisioning Originating Host Class Profile routing for BGCF, [4-160](#)
- Provisioning subscriber profile routing for BGCF, [4-163](#)
- 
- Provisioning Support of the NENA V5 SIP Interface to LRF and EATF for SRVCC, [1-92](#)
- provisioning task flow
- ACR, [3-3](#)
  - IMS-GWF, [1-30](#)
- Provisioning task flow
- Multiple Destination FQDNs, [1-36](#)
- provisioning task flow
- NASS-bundled authentication, [1-43](#)
- Provisioning task flow
- Priority Mode, [1-49](#)
- Provisioning task flow - To provision P-CSCF pool, [4-126](#)
- S-CSCF Pool, [4-40](#)
- SIP heartbeat after failure to reach a network element, [1-123](#)
- SIP Message Screening, [1-47](#)
- Support Primary and Alternate SLF Destination for Geo-Redundancy, [1-125](#)
- Provisioning Task flow - Support New Versions of IMS Charging SPEC 3GPP 32.260, [1-127](#)
- Provisioning the Subscriber Home Domain Table, [5-281](#)
- published NI IP addresses for FEPH and IMS service, [5-161](#)
- 
- R remove FEPH capability for IMS service, [5-170](#)
- Routing
- provision incoming digit table, [10-50](#)
- 
- wildcards in digit strings, [10-68](#)
- S** S-CSCF profile
- online charging, [9-7](#)
- Safety
- basic aspects of, [12-6](#)
- SB Server
- Parameters, [10-9](#)
- SCTP Parameter Profile
- add, modify, or delete, [10-37](#)
- SDP media provisioning, [4-6](#)
- SEAL
- Configuration, [5-159](#)
- Service Policy Decision Function
- To provision an IP Filter table, [7-6](#)
- Service Route
- header, [4-102](#)
- Sigcomp
- SIP compression provisioning, [4-69, 4-106](#)
- Signaling Firewall Load Balancer or Distribution Function with Single IP Address Exposed for the Gm Interface to End Users - Provisioning Taskflow, [1-64](#)
- Signaling Firewall Service Growth with existing IMS Services, [5-172](#)
- SIP
- Activate, [8-3](#)
  - Provisioning, [4-102](#)
  - Signaling compression provisioning, [4-69, 4-106](#)

|  |   |  |
|--|---|--|
| SIP Error Treatment Attributes   | TLS Profile Attributes  | Variants   |
| Provisioning the SIP Error Treatment Table attributes, <a href="#">4-123</a>   | Provisioning, <a href="#">4-121</a>   | Administer PPL components, <a href="#">10-116</a>              |
| SIP Linkset  | To add, modify or delete an S-CSCF profile, <a href="#">4-15</a>                | View administrative state of SIPia port, <a href="#">10-83</a> |
| add, modify, or delete, <a href="#">4-264</a>  | To assign a Published Realm to a Border Gateway, <a href="#">4-290</a>          | View operational state   |
| SIP Message Screening  | To connect to the CNFG host using the Provisioning GUI, <a href="#">10-4</a>    | IMS Service, <a href="#">10-82</a>                             |
| provisioning task flow, <a href="#">1-47</a>   | To convert one ordinary subnet to external access subnet, <a href="#">5-360</a> |  |
| SIP Permanent Linkset  | To degrow one external access subnet, <a href="#">5-371</a>                     |  |
| Provisioning task flow, <a href="#">1-35</a>   | To grow a new external access subnet, <a href="#">5-343</a>                     |  |
| SIP Permanent Linkset Group  | To provision  |  |
| add, modify, or delete, <a href="#">4-269</a>  | SIP Filter, <a href="#">5-23</a>  |  |
| SIPia  | SIP Filter Body Rule, <a href="#">5-36</a>                                      |  |
| SIP compression, <a href="#">4-69</a> , <a href="#">4-106</a>  | SIP Filter Header Rule, <a href="#">5-28</a>                                    |  |
| SIPia port   | To provision a DSCP profile table, <a href="#">7-36</a>                         |  |
| add, modify, or delete, <a href="#">10-40</a>  | To provision a FEPH Flow Policy, <a href="#">5-142</a>                          |  |
| SIPia port state   | To provision an ACR Charging Profile, <a href="#">8-5</a>                       |  |
| for FS GUI, <a href="#">10-80</a>  | To provision an E-CSCF Profile table, <a href="#">4-212</a>                     |  |
| FS GUI, <a href="#">10-83</a>  | To provision an E.164 Expansion AS profile, <a href="#">4-238</a>               |  |
| SIPia status on Alcatel-Lucent CP, <a href="#">10-80</a>   | To provision an IPsec Parameters table, <a href="#">5-155</a>                   |  |
| Support collecting Bearer statistics at AGCF from Access GW, <a href="#">5-123</a>                                     | To provision an Originating Hosts table, <a href="#">10-64</a>                  |  |
| Support Multiple Access Network Subnets on FEPH, <a href="#">5-342</a>   | To provision an SCTP Parameter profile  |  |
| Support sending offline charging data to the CCF provisioned to the CTS, <a href="#">5-264</a>                         | SCTP Profile, <a href="#">10-37</a>   |  |
| Support sending offline charging data to the CCF provisioned to the CTS - Provisioning task flow, <a href="#">1-80</a> |   |  |
| Support to provide P-CSCF IP address to UE, <a href="#">4-120</a>  |   |  |

**T** task flowe2 interface support, [4-116](#)**V** VariantProvisioning, [10-114](#)